Link1000ACS
Wireless Web Interface

User's Guide

icXchange®

www.intcomcorp.com

This is the Link1000ACS Wireless Web Interface User's Manual. It contains instructions to configure the wireless components of the Link1000ACS Access Control Switch and any of its associated access points (AP).

Intended audience

This manual is designed to be used by network managers, administrators, and technicians who are responsible for installing networking equipment in enterprise and service provider environments. Knowledge of telecommunication and Internet protocol (IP) technologies and advanced knowledge of LAN/WLAN networking is assumed.

Documentation

icXchange® product and support documentation consists of a variety of manuals, installation guides, videos, knowledge articles, sample designs, and troubleshooting and FAQ guides to assist you with the deployment of your new and innovative solution.

These and other documents are available for download at http://intcomcorp.com/education-support.html.

To view PDF files, use Adobe Acrobat Reader® 5.0 or newer. Download Acrobat Reader® for free from the Adobe website: www.adobe.com/products.

Contact information

Phone: (888) OPT.LINK
E-mail: support@intcomcorp.com
sales@intcomcorp.com

Icons

Table of Contents

Contact

Previous Page

Next Page

Safety precautions

For safe and efficient use, read the following information.

Text conventions

Table 0-1: Text conventions

Icon	Description
NOTE	Emphasizes information to improve product use.
IMPORTANT	Indicates important information or instructions that must be followed.
CAUTION	Indicates how to avoid equipment damage or faulty application.
WARNING	Issues warnings to avoid personal injury.

Below is a listing of safety precautions and definitions.

Table 0-2: Safety precautions

Icon	Description
WARNING	Before working on this equipment, be aware of good safety practices and the hazards involved with electrical circuits.
WARNING	To reduce risk of fire hazard and electric shock, do not install the unit near a damp location.
CAUTION	To reduce the risk of fire, use only number 26 AWG or larger UL Listed or CSA Certified telecommunication line cord for all network and telecommunication connections.

- Keep the product in a clean and dust-free location. Use only a soft, damp cloth to clean the product.
- DO NOT expose the product to liquid or moisture.
- DO NOT expose the product to extreme temperatures.

Table of contents

Intended audience i
Documentation i
Contact information i
Icons i

Safety precautions ii
Text conventions ii

Table of contents iii

Chapter 1: Introduction to Web page configuration 1
1.1 Configuration preparation 1
1.1.1 Computer requirements 1
1.1.2 The Link1000ACS management through Web 1
1.2 Web interface introduction 5
1.2.1 Log in to the Link1000ACS 5
1.2.2 Web interface introduction 5
1.2.3 Menu introduction 6
1.2.4 Exiting the Web interface of the Link1000ACS 9

Chapter 2: Dashboard 10
2.1 System info 10
2.2 Managed access point 11
2.3 Device info 11
2.4 Support 11

Chapter 3: Fast configuration 12
3.1 IP configuration 12
3.2 AP group configuration 13
3.3 Network configuration 13
3.3.1 SSID 13
3.3.2 Security 14

Chapter 4: System configuration 16
4.1 WLAN enable 16
4.2 Auto IP assign mode 17
4.3 AP authentication mode 17
4.4 AP validation method 18
4.5 Radius authentication server 18
4.6 Radius accounting mode 18
4.7 Radius accounting server 19
4.8 Client-QoS global mode 19
4.9 Country code 19
4.10 Peer group ID 19
4.11 Cluster priority 20

Chapter 5: Networks 21
5.1 Configure network ID 21
5.2 Configure authentication mode 21
5.2.1 Open authentication mode 21
5.2.2 Static WEP authentication mode 21
5.2.3 WEP 802.1x 22
5.2.4 WPA personal 23
5.2.5 WPA enterprise 23
5.3 Configure VLAN 24
5.4 MAC authentication 24
5.5 Portal instance 24
5.6 Client QoS 25

Chapter 6: AP group management 26
6.1 Add/modify/delete AP group 26
6.1.1 Normal attribute 27
6.1.2 AP configuration 27
6.1.3 Radio 29

6.1.4 VAP 29
6.1.5 QoS 30
6.1.6 TSPEC 31
6.2 Copy AP group 32
6.3 Apply AP group 33

Chapter 7: Security authentication 34
7.1 Radius configuration 34
7.1.1 Global configuration 34
7.1.2 Radius authentication server configuration 35
7.1.3 Radius accounting server configuration 35
7.1.4 Radius group manage 36
7.1.5 Radius configuration 36
7.2 LDAP configuration 37

Chapter 8: Discovery 39
8.1 IP discovery 39
8.1.1 Enable and disable IP discovery 39
8.1.2 Add IP of L3/IP discovery 39
8.1.3 Delete IP address from L3/IP discovery list 39
8.2 L2 VLAN discovery 40
8.2.1 Enable L2 VLAN discovery 40
8.2.2 Add VLAN of L2/VLAN discovery 40
8.2.3 Delete VLAN from L2 VLAN discovery list 40

Chapter 9: Provisioning 41
9.1 AP provisioning 41
9.2 AC provisioning 42
9.3 Mutual authentication 43

Chapter 10: Provisioning over NAT 44
10.1 NAT provisioning configuration 45
10.1.1 NAT ports 45
10.1.2 Access point NAT configuration 45
10.2 Link1000ACS access controller NAT configuration 46
10.2.1 NAT ports 46
10.2.2 Link1000ACS NAT configuration 46

Chapter 11: WIDS security 48
11.1 WIDS AP configuration 49
11.2 WIDS client configuration 51
11.3 Known client 53
11.3.1 MAC authentication mode 53
11.3.2 Black/white list configuration 54

Chapter 12: Captive portal 55
12.1 Global configuration 55
12.2 Captive portal authentication type 56
12.3 Portal server configuration 56
12.4 Free resource configuration 57
12.5 MAC portal configuration 58
12.6 Portal instance configuration 59

Chapter 13: Configuration push 61
13.1 Configuration push 61
13.2 Configuration push option 61

Chapter 14: AP image upgrade 63
14.1 AP manual upgrade configuration 63

Chapter 15: Load balance 68
15.1 Create template 68
15.2 AP profile associated load balance template 69
15.3 Delete load balance template 69

Chapter 16: Data transfer 70
16.1 Centralized L2 tunnel configuration 70
16.1.1 VLAN config 70

16.1.2 Station isolation VLAN 71

Chapter 17: Time limit policy 72
17.1 Network time limit configuration 72
17.2 Radio time limit configuration 73

Chapter 18: Organization unique identifier (OUI) 75
18.1 Add OUI 75
18.2 Delete OUI 75

Chapter 19: Trap and syslog 76
19.1 SNMP traps 76
19.1.1 Wireless global traps 76
19.2 Syslog configuration 77
19.2.1 Wireless syslog configuration 77
19.2.2 Captive portal syslog configuration 77

Chapter 20: Monitor 78
20.1 AC 78
20.1.1 Cluster 79
20.1.2 Each AC status/statistics 83
20.2 AP 85
20.2.1 Basic AP information 86
20.2.2 AP detail 86
20.2.3 Failure AP list 91
20.3 Wireless client 92
20.3.1 Associated client list 92
20.3.2 Associated client detail 93
20.3.3 Detected client list 95
20.3.4 Detected client detail 96
20.4 RF scan 98
20.4.1 AP RF scan status 98
20.4.2 AP RF scan detail 98
20.4.3 Client dynamic blacklist 101

Chapter 21: Management 102
21.1 Basic configuration 102
21.1.1 Login user configuration 102
21.1.2 Login user authentication method configuration 103
21.1.3 Login user security IP management 104
21.1.4 Basic configuration 105
21.1.5 Save current running-configuration 106
21.2 SNMP configuration 107
21.2.1 SNMP Authentication 107
21.2.2 SNMP management 111
21.2.3 Community managers 112
21.2.4 Configure SNMP manager security IP 114
21.2.5 SNMP Statistics 114
21.3 SSH management 115
21.3.1 Switch on-off SSH 115
21.3.2 SSH management 116
21.4 Firmware update 117
21.4.1 TFTP client service 118
21.4.2 TFTP server service 119
21.4.3 FTP client service 119
21.4.4 FTP server service 121
21.5 Telnet server configuration 122
21.5.1 Telnet server state 122
21.5.2 Max numbers of telnet access connection 123
21.6 Maintenance and debugging command 123
21.6.1 Debug command 124
21.6.2 Others 125

Regulatory and compliance 127

Warranty 130

Chapter 1: Introduction to Web page configuration

This chapter details the Web configuration page.

1.1 Configuration preparation

Manage the Link1000ACS by connecting to the Web via an Ethernet interface.

1.1.1 Computer requirements

- Compatible operating systems (Win XP®/Win 7®/Win 8®/Mac OS® 10.6/7)
- Web browser (IE 8/9/10/11, Google Chrome™, Firefox®, Safari®)

1.1.2 The Link1000ACS management through Web

To configure the Link1000ACS locally, the PC's and the Link1000ACS's IP addresses should be configured in the same subnet. The Link1000ACS default IP address is 192.168.1.1, and the subnet mask is 255.255.255.0.

The following are steps to create a network connection.

Step 1: Set up the environment.

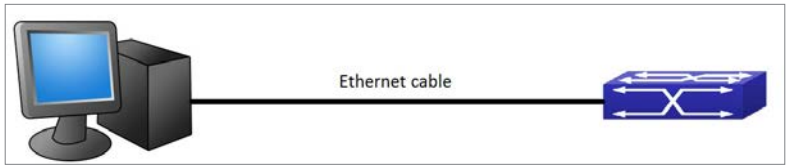


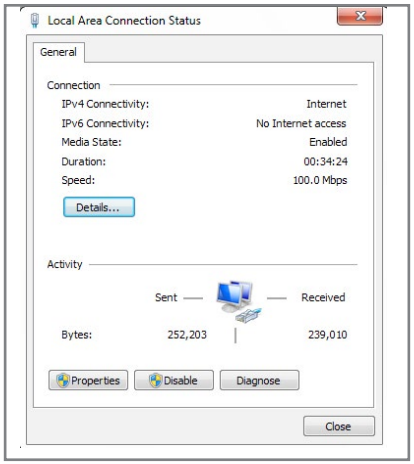
Figure 1-1: Web management configuration environment

Connect the PC Ethernet port to the Link1000ACS Ethernet port with an Ethernet cable.

Step 2: Set up the network connection (as shown with Windows 7®).

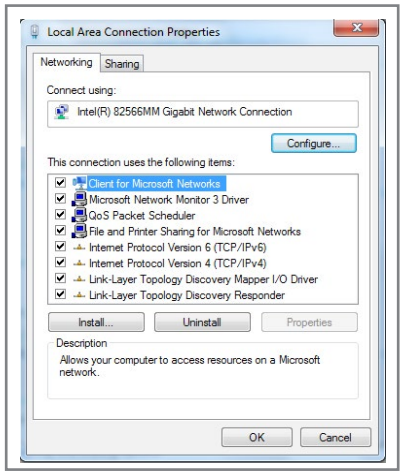
Click **Start**. Select **Control Panel**. Click **View network status and tasks**, and then click **Local Area Connection**. The **Local Area Connection Status** dialog box will appear, as shown in Figure 1-2.

Figure 1-2: Local area connection status



Click **Properties** to open the **Local Area Connection Properties** dialog box, as shown in Figure 1-3.

Figure 1-3: Local area connection properties



Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties** to open the **Internet Protocol (TCP/IP) Properties** dialog box. Select **Use the following IP address**, type the IP address (between 192.168.1.2 and 192.168.1.254) and the subnet mask (255.255.255.0), then click **OK**.

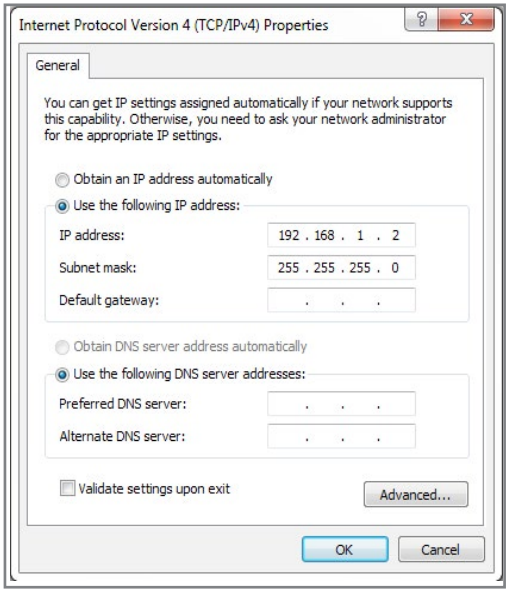

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Figure 1-4: Internet protocol (TCP/IP) properties

Step 3: Use **PING** command to ensure the connection status between the PC and the Link1000ACS.

Click **Start**, and then type **CMD** in the text box. Press **ENTER** to generate the Command Prompt window. Type ping **192.168.1.1** (the Link1000ACS's default IP address), and then press **ENTER**. If the network is connected, the window will include the following text (Figure 1-5).

If this text is not shown, confirm the network connection is plugged in properly, the Ethernet cable is functioning properly, and that the PC has the correct IP address, as configured previously.

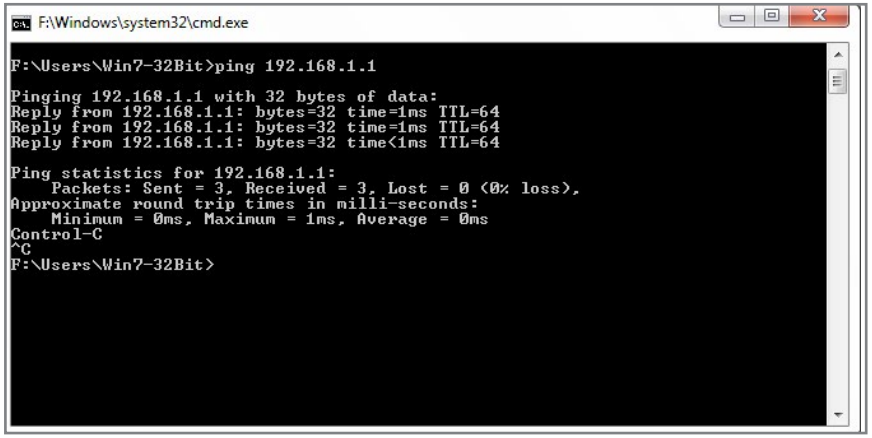

F:\Windows\system32\cmd.exe
F:\Users\Win7-32Bit>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
F:\Users\Win7-32Bit>

Figure 1-5: Dialog box for command lines

Step 4: Cancel proxy server.

If the current PC uses the proxy server to access the Internet, the proxy server must be disabled. Complete the following steps to disable the proxy server:

1. In Internet Explorer, select **Tools,** and then select **Internet Options** to open the Internet Options window.
2. Select **Connections** in the Internet Options window, and then click **LAN Settings** to open the **Local Area Network (LAN) Settings** dialog box, as shown in Figure 1-6.

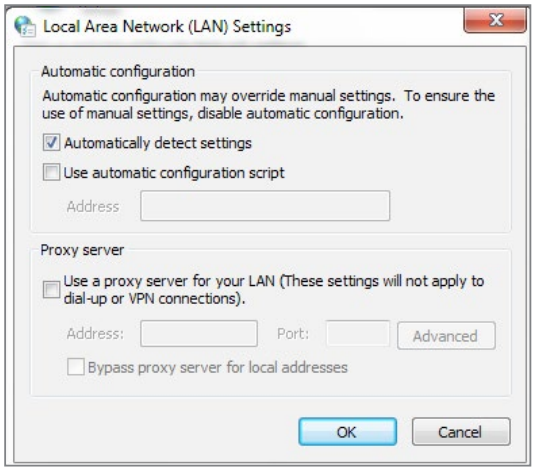

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced
Bypass proxy server for local addresses
OK
Cancel

Figure 1-6: Local area network (LAN) settings

3. Ensure that **Use a proxy server for your LAN** is not selected. Otherwise, clear the selection, and then click **OK**.

1.2 Web interface introduction

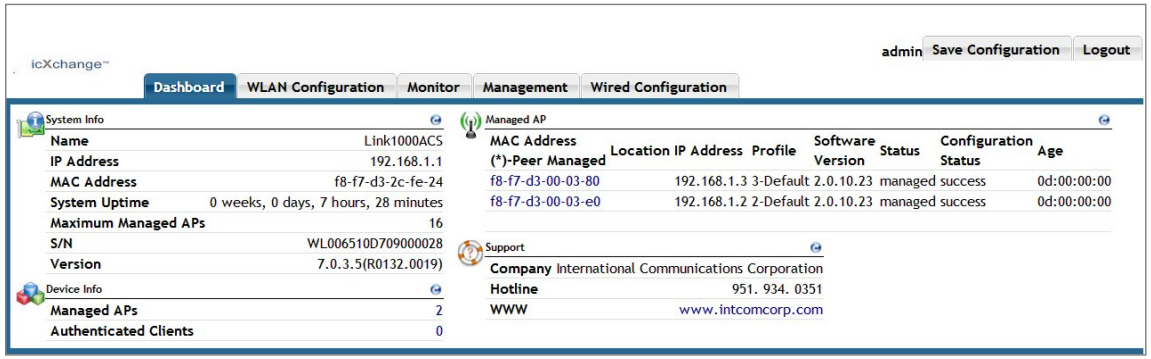
1.2.1 Log in to the Link1000ACS

Open the Web browser, type the IP address **192.168.1.1** in the address bar, and press **ENTER** to open the login page for the Link1000ACS. Type the username and password (the default username is **admin**, and the password is **admin**), click **Login**, or press **ENTER** to open the **Web Configuration** page. The figure is shown as follows:

1.2.2 Web interface introduction

Upon logging in, the dashboard will appear, showing the basic information of the current Link1000ACS and the managed AP status. Chapter 2 provides a detailed introduction to the dashboard.

At the top of the screen are tabs for each functional module. Click the corresponding tab to configure the wireless or wired functions.



1.2.3 Menu introduction

On the top right of the main Graphical User Interface (GUI) screen there are three fields; **user account name**, **Save Configuration** and **Logout**.

- user account name - The name of the user's login account. Admin will be displayed if the user is logged in under an admin account. A user can create multiple login accounts with various privilege levels as discussed in Chapter 21.
- Save Configuration – Click **Save Configuration** to retain the running configuration. This saved configuration will be used by the Link1000ACS after a reboot.
- Logout – Click **Logout** to exit the current configuration session.

Users can check the connected configuration interface function with each menu option, as noted in the following table.

Menu	Page	Page Function
Dashboard		
WLAN configuration	Fast Configuration	
	System Configuration	
	Networks	
	AP Group Management	
	Security Authentication	
	Discovery	
	Provisioning	
	WIDS Security	
	Captive Portal	
	Advanced Configuration	Configuration Push
		AP Image Upgrade
		Load Balance
		Data Transfer
		Time Limit Policy
		Organization Unique Identifier (OUI)
		Trap and Syslog
Monitor	AC	
	AP	
	Wireless Client	
	RF Scan	

Menu	Page	Page Function
Management	Switch Basic Configuration	Login User Configuration
		Login User Authentication Method Configuration
		Login User Security IP Management
		Basic Configuration
		Save Current Running-Configuration
	SNMP Configuration	SNMP Authentication
		SNMP Management
		Community Managers
		Configure SNMP Manager Security IP
		SNMP Statistics
	SSH Management	Switch on-off SSH
		SSH Management
	Firmware Update	TFTP Service
		FTP Service
	Telnet Server Configuration	Telnet Server State
		Max Numbers of Telnet Access Connection
	Maintenance and Debugging Command	Debug Command
		Show Clock
		Show CPU Usage
		Show Memory Usage
		Show Flash
		Show Running-config
		Show Switchport Interface
		ShowTCP
		Show UDP
		Show Telnet Login
		Show Version

1.2.4 Exiting the Web interface of the Link1000ACS

Click **Logout** to exit and return to the **Login** page.

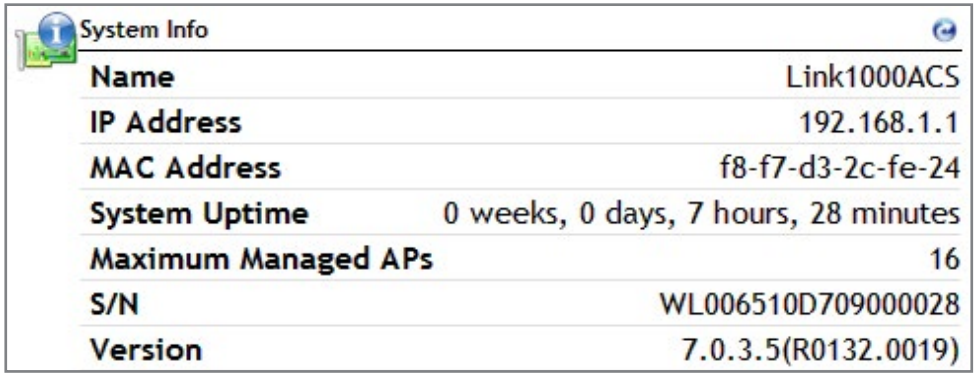
The chapters that follow describe how to enable and configure various features offered by the icXchange® solution. To properly access the advanced configuration options for a particular feature, the feature must first be enabled by following the configuration steps for that feature as described in this user manual. If the feature is not enabled, users may not be able to perform advanced configuration for that feature. Warning messages may be displayed identifying that the feature must first be enabled before the configuration can be completed.

Chapter 2: Dashboard

The dashboard includes four parts: **System Info, Managed AP, Device Info**, and **Support**.

2.1 System info

System Info for the Link1000ACS is as follows:

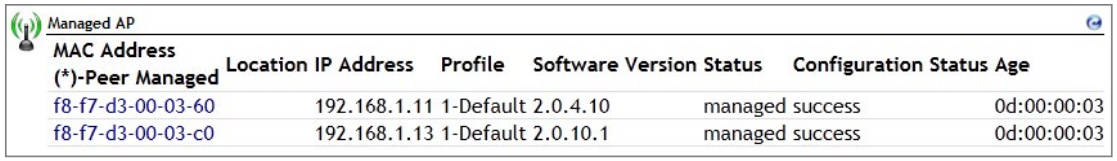


The information in the figure is as follows:

- Name: the name of the Link1000ACS is Link1000ACS.
- IP Address: the wireless address of the Link1000ACS is 192.168.1.1.
- MAC Address: the MAC address of the Link1000ACS is f8-f7-d3-2c-fe-24.
- System Uptime: the normal running time: 1 day, 4 hours, and 2 minutes.
- Maximum Managed APs: 16.
- S/N: WLD006510D709000028.
- Version: 7.0.3.0(R0041.0019).
- : click to refresh the information.

2.2 Managed access point

Managed AP shows the **MAC Address**, **Location**, **IP Address**, **Profile**, **Software Version, Status, Configuration Status** and **Age**.

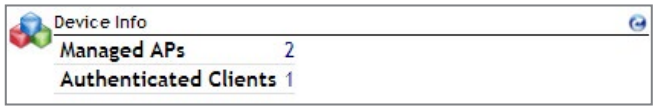


- MAC Address: AP's MAC address
- Location: location of AP
- IP Address: IP address of AP
- Profile: profile that the AP belongs to
- Software Version: version of AP
- Status: AP's current management status
- Configuration Status: AP's current configuration status
- Age: AP keep alive age - will only increment on AP failure

Click the AP's MAC address to access the **Detailed AP List** page.

2.3 Device info

Device Info displays the total number of managed APs and authenticated clients in the cluster.



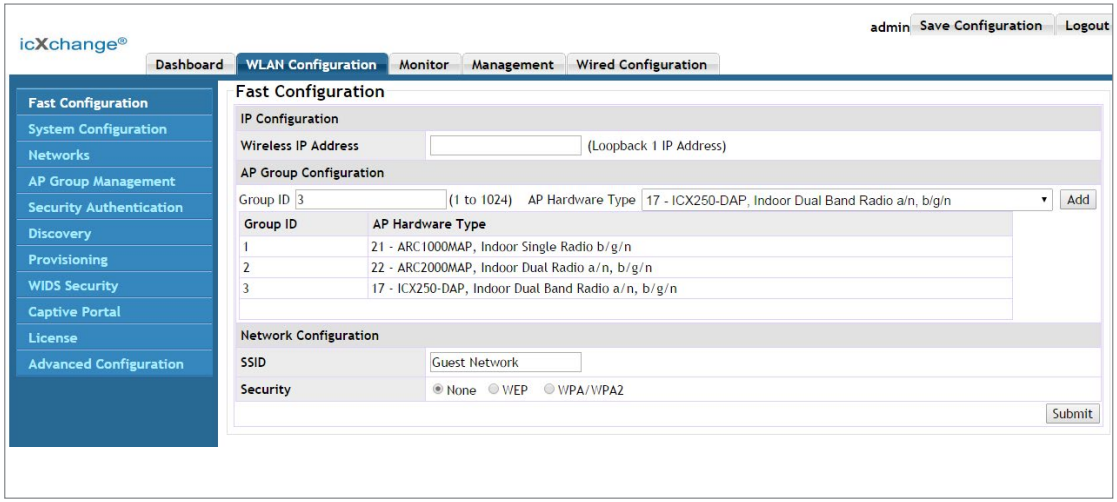
2.4 Support

Support provides the company's email address, hotline phone number, and the website address.

Chapter 3: Fast configuration

Click **WLAN Configuration->Fast Configuration** to configure the WLAN functions, including the WLAN managed IP address, AP groups, and the basic network configuration. This configuration is submitted to the Link1000ACS.

Note: **Fast Configuration** is a simple way to perform initial configurations on the Link1000ACS. However, using the **Fast Configuration** option will overwrite all previous configurations that were previously configured on the Link1000ACS.



3.1 IP configuration

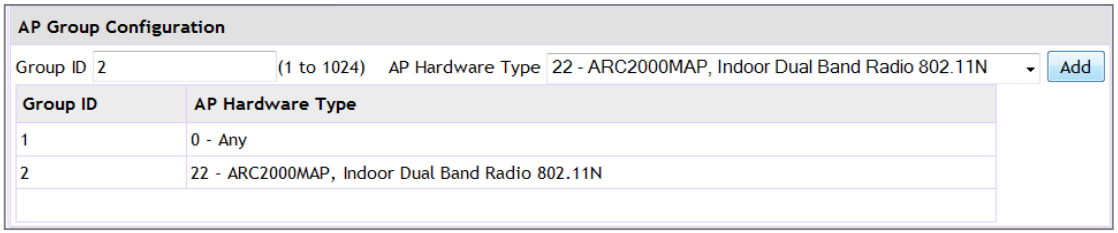
IP Configuration is used to configure the wireless IP address. Type the wireless IP address. The IP address entered will be configured as the wireless IP address.

3.2 AP group configuration

AP Group Configuration adds and updates the ID and hardware type of the AP group.

Example: Type **2** in the Group ID box. Select **22 - ARC2000MAP, Indoor Dual Band Radio 802.11N** as the corresponding AP Hardware Type, and then click **Add** to add them to the page.

Note: You must click **Submit** after entering all information on the Fast Configuration page to save the configuration to the Link1000ACS, or the modification will be lost.



3.3 Network configuration

Network Configuration configures the network used by AP. The network configuration can configure SSID and security settings for Network1, which are applied to the VAP for all AP groups.

3.3.1 SSID

SSID is the service set mark of the WLAN; in this example, it is the name of the WLAN. SSID can divide one WLAN into subnets that need different ID authentication. Only the user who passes the ID authentication can access the corresponding subnet. It can prevent users without appropriate permissions from accessing this network.

Example: Type the name of the network in the SSID box, such as **Network1**. Select **None** for Security. Click **Submit**.

3.3.2 Security

Security can configure the access control of the security authentication. The methods of authentication include **Static WEP**, **WEP IEEE802.1x**, **WPA/WPA2 Personal**, and **WPA/WPA2 Enterprise**.

3.3.2.1 WEP mode

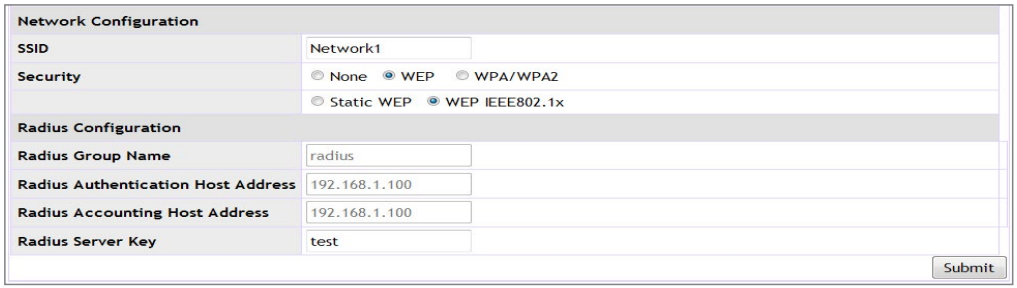
Select **WEP** to access the quick WEP authentication configuration. Under WEP, there are two types of modes: **Static WEP** and **WEP IEEE802.1x**.

Static WEP has the same configuration as **WLAN Configuration->Network Config** (detailed in Chapter 5: Networks).

Select **WEP IEEE802.1x** to configure it.

Example: Type the Radius Group Name as **radius**. Type the Authentication Host Address and Accounting Host Address as **192.168.1.100**. Enter the Radius Server Key that corresponds to the Key set on the configured radius server, and then click **Submit**.

Note: Only the RADIUS authentication and accounting server without configuration can be configured in **Fast Configuration**. If they were already configured, they cannot be deleted or modified in the configuration (detailed in Chapter 7: Security authentication).



3.3.2.2 WPA/WPA2

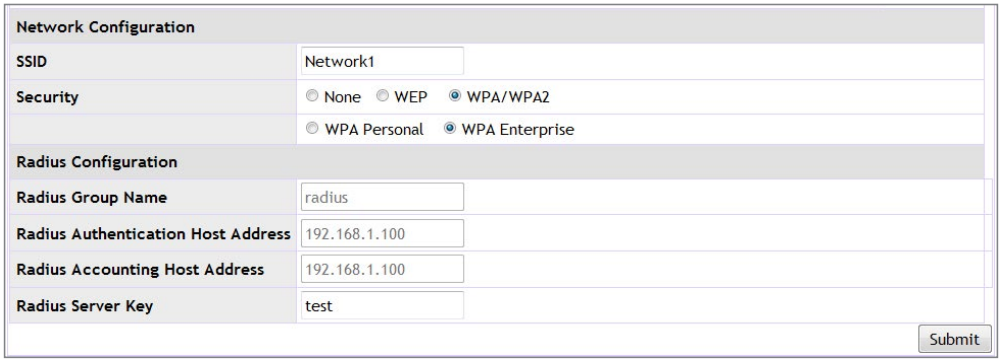
Select **WPA/WPA2** to configure the WPA/WPA2 authentication. There are two modes: **WPA Personal** and **WPA Enterprise**.

Configuration for WPA personal is the same as **WLAN Configuration->Networks->WPA Personal** (detailed in Chapter 5: Networks).

WPA Enterprise has the same configuration as WEP 802.1x. Choose the **WPA Enterprise** button to enter into the configuration.

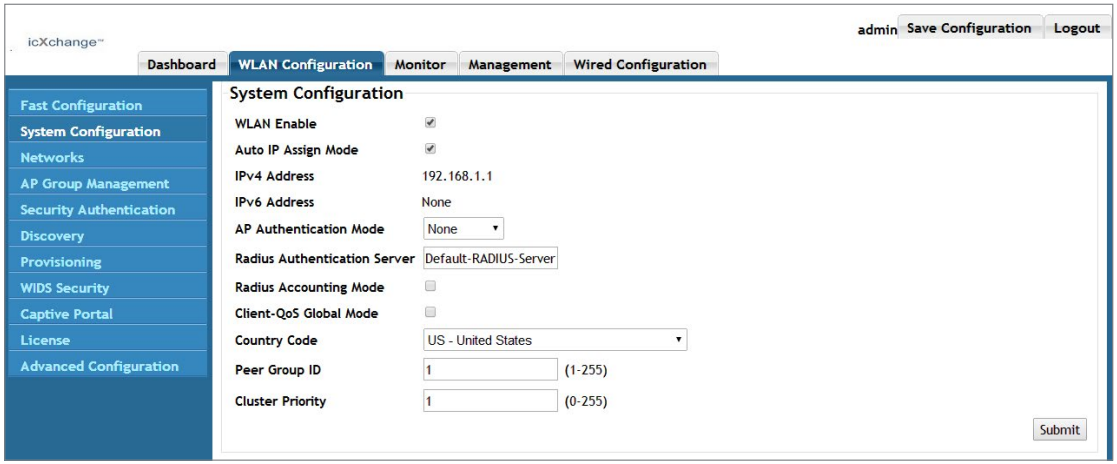
Example: Type the Radius as **radius**. Type the Authentication Host Address and Accounting Host Address as **192.168.1.100**. Enter the Radius Server Key that corresponds to the Key set on the configured radius server, and then click **Submit**.

Note: Only the Radius authentication and billing server without configuration can be configured in **Fast Configuration**. If they were already configured, they cannot be deleted or modified in **Fast Configuration** (detailed in Chapter 7: Security authentication).



Chapter 4: System configuration

Click **WLAN Configuration->System Configuration** to open the **System Configuration** page. From this page, the corresponding parameters under WLAN global mode can be configured. The figure is as follows:



4.1 WLAN enable

Select **WLAN Enable** to enable the WLAN function. The Link1000ACS WLAN service can only be used after selecting this option. If it is not selected, all WLAN functions on the Link1000ACS will be disabled, and WLAN service will be stopped.

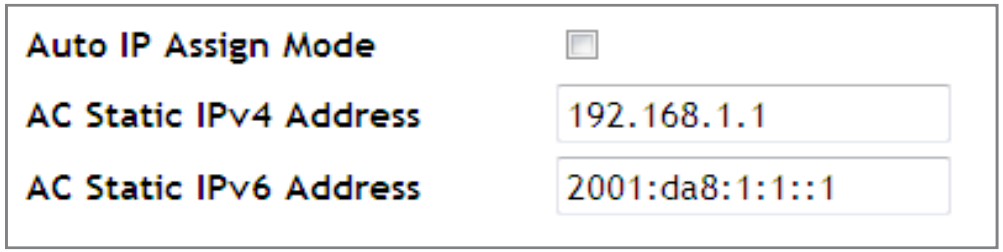
Note: Default setting is WLAN disable. **Fast Configuration** will automatically update to WLAN enabled.

4.2 Auto IP assign mode

Select **Auto IP Assign Mode**, allowing the WLAN function to choose the IP address automatically.

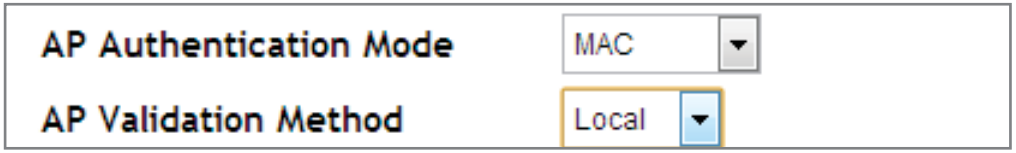
When enabled, APs can have automatic IP address assignment from the Link1000ACS Wireless IP subnet. If the user has configured multiple Layer-3 interfaces or loopback interfaces on the controller, select the WLAN IP address to be the lowest IP address among the Layer-3 interface subnets or the lowest loopback interface.

Clear the **Auto IP Assign Mode** check box to disable the auto IP assign mode, and then type a static IP address manually. When configuring the static IP, the address of the existing loopback or L3 interfaces should be chosen; otherwise, it will not be effective, and the WLAN function will not function properly.



4.3 AP authentication mode

There are three modes of AP authentication. **MAC** is the default mode.



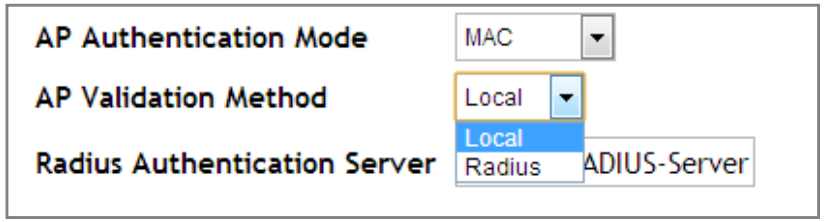
None sets the automatic registration authentication mode. The AP database does not need to be added manually on the Link1000ACS. It can join the cluster when the Link1000ACS or the AP automatically connects.

MAC sets the MAC address authentication mode. The AP database needs to be set manually, and then the AP can join the Link1000ACS.

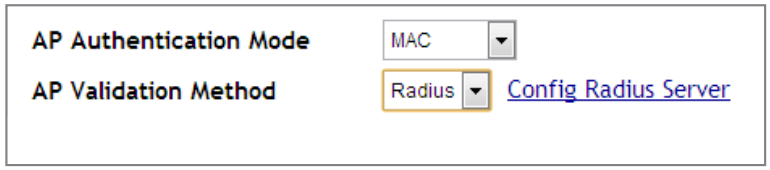
Password sets the password authentication mode. After the TLS connection is created between the AP and the Link1000ACS, they can join the cluster through password authentication.

4.4 AP validation method

If **MAC** is selected for the AP authentication mode, the AP validation method can be configured. This option allows either local authentication or RADIUS server authentication for AP authentication. **Local** authentication is default. The authentication method can be changed to be RADIUS server authentication by selecting **Radius** from the **AP Validation Method** drop-down list.



If **Radius** is selected, the user must choose a server name from the Radius server group list (it should be configured first, as shown in Chapter 7: Security authentication). The authentication request will be sent to the selected Radius server.

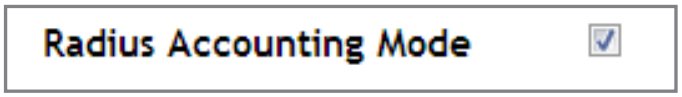


4.5 Radius authentication server

Configure the Radius authentication server by typing **radius**.

4.6 Radius accounting mode

Select the **Radius Accounting Mode** check box to enable the Radius accounting function.



4.7 Radius accounting server

Configure the Radius Accounting Server by typing **RADIUS-Server**.

4.8 Client-QoS global mode

Select the **Client-QoS Global Mode** check box to enable the global client-QoS function of the Link1000ACS.

Client-QoS Global Mode is divided into **global on-off** and **current network on-off**. Both should be enabled so that clients associated with this network and the configured ACL, DiffServ, and rate limit of down/up can be used.

4.9 Country code

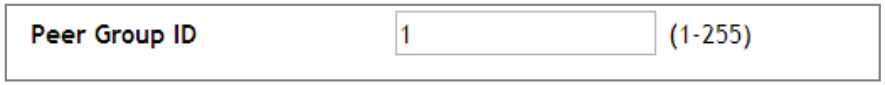
The **Country Code** drop-down list is used to configure the country code of the Link1000ACS and AP. **US – United States** is the default.

The configured country code must conform to the country of the device's location due to the necessary lawful channels of different countries.

4.10 Peer group ID

The cluster mark can be configured through this **Peer Group ID** text box. The Link1000ACSs with the same group ID can create a WLAN cluster and transmit information to each other. The Link1000ACSs with different group IDs cannot communicate with each other.

The default peer group ID is 1, and the range is from 1 to 255.



4.11 Cluster priority

The **Cluster Priority** text box appoints the priority of selecting the Link1000ACS Access Control Switch for the Link1000ACS.

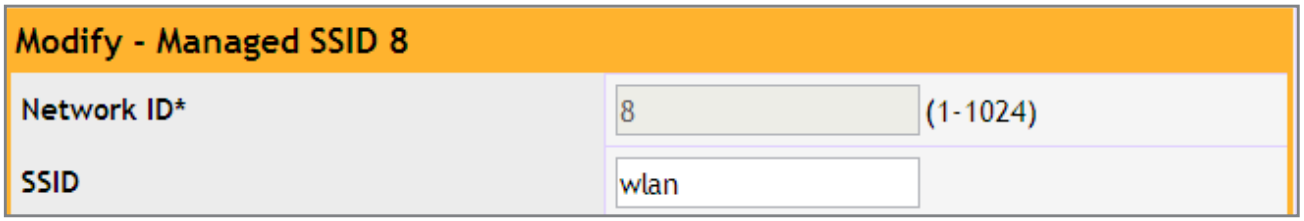
The higher the value, the higher the priority. This Link1000ACS can easily be selected as the access control switch. When changing the priority of one Link1000ACS in a cluster, the new selection of the Link1000ACS Access Control Switch will be triggered.

The default cluster priority is 1, and the range is from 0 to 255.

Chapter 5: Networks

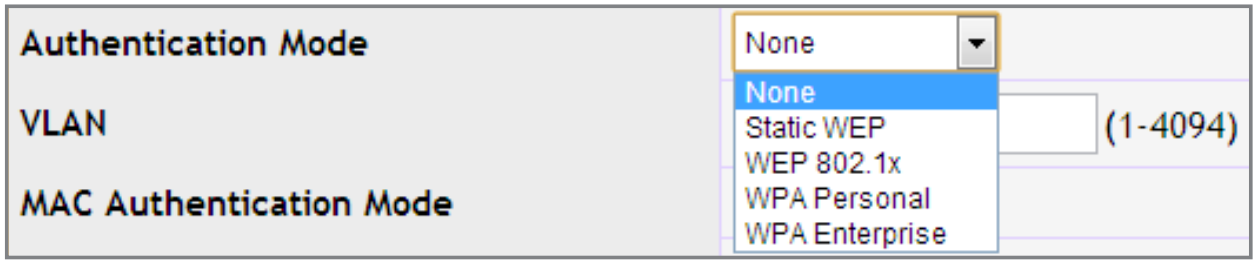
5.1 Configure network ID

The default network ID is network1. Either select the existing network to configure, or create a new network. Click **WLAN Configuration ->Networks**, and choose a network. For example, modify the SSID of network 8 as **wlan**.



5.2 Configure authentication mode

The network includes multiple authentication modes.



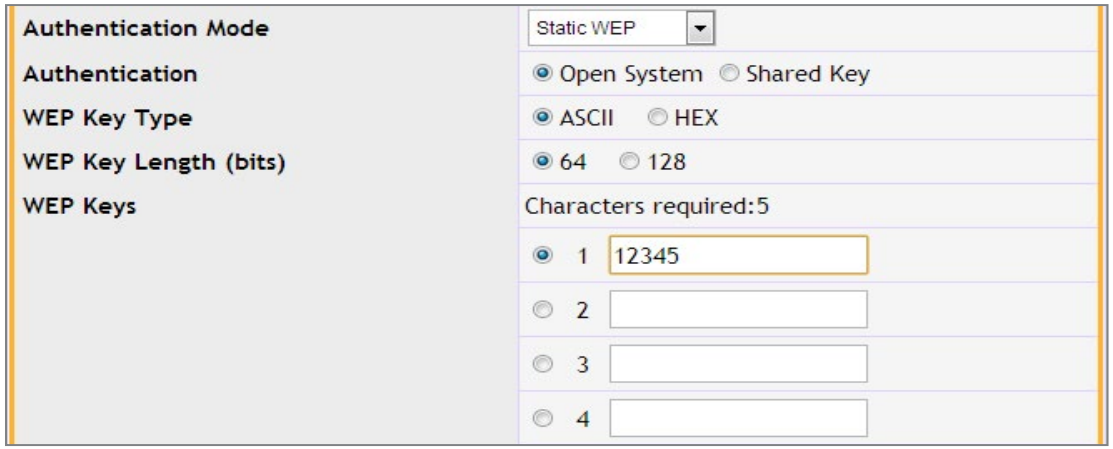
5.2.1 Open authentication mode

None sets the authentication mode as **open**. The corresponding command is **security mode none**, meaning the username and password are not needed to associate with the network, and the authentication will be successful.

5.2.2 Static WEP authentication mode

Static WEP sets the authentication mode as **security mode static-wep**. The WEP key is needed when connecting to the network. The WEP authentication mode includes **open system** and **shared key**. The WEP key type includes **ASCII** and **HEX**. The length includes 64-bit and 128-bit security.

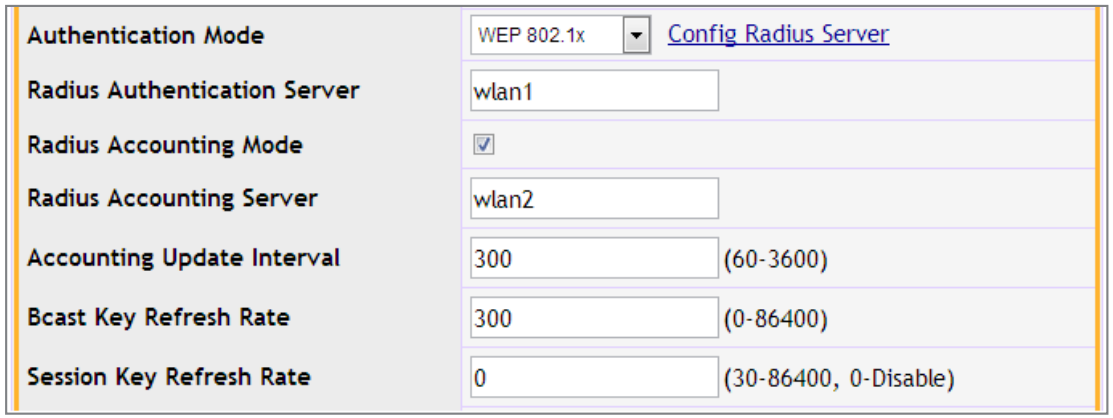
Example: Select the Authentication as **Open System**, the WEP Key Type as **ASCII**, and the Length as **64**. Type the WEP Key as **12345**. The figure is as follows:



5.2.3 WEP 802.1x

WEP 802.1x sets the configuration as **security mode wep-dot1x**. This authentication mode needs the radius server's WEP authentication. To configure WEP 802.1x please refer to Chapter 7: Security authentication, Radius authentication server configuration.

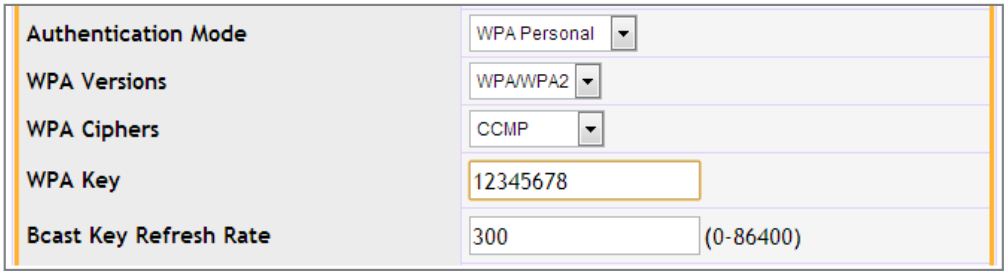
Example: Type the Radius Authentication Server as **wlan1**, and type the Radius Accounting Server as **wlan2**. The Accounting Update Interval, Bcast Key Refresh Rate, and Session Key Refresh Rate adopt the default WEP 802.1x authentication. Click **OK**. The figure is as follows:



5.2.4 WPA personal

WPA Personal sets the configuration as **security mode wpa-personal**. It requires the WPA password for the association when connecting to the network. There are three modes: **WPA, WPA2**, and **WPA/WPA2**. There are two WPA ciphers: **TKIP** and **CCMP**.

Example: Select **WPA Personal** from the **Authentication Mode** drop-down list, select **WPA/WPA2** from the **WPA Versions** drop-down list, select **CCMP** from the **WPA Ciphers** drop-down list, type **12345678** in the **WPA Key** field, and type **300** in the **Bcast Key Refresh Rate** field. Click **OK**.

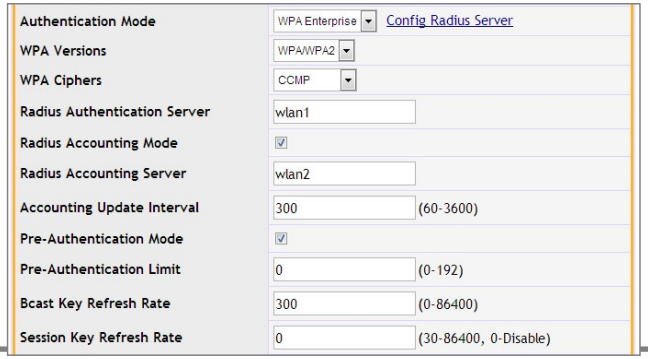


5.2.5 WPA enterprise

WPA Enterprise sets the configuration as **security mode wpa-enterprise**. It authenticates and accounts through the Radius server. The cipher and WPA version in WPA enterprise are the same as in the cipher and WPA version in WPA personal. However, WPA enterprise requires Radius server authentication. Prior to Radius server authentication, users can pre-authenticate. Click **Config Radius Server** to enable it.

When the client associates in **WPA Enterprise** mode, valid username and password are required through the Radius server.

Example: Select the WPA Versions as **WPA/WPA2** and the WPA Ciphers as **CCMP**. Type the Radius Authentication Server as **wlan1**, and type the Radius Accounting Server as **wlan2** (the detailed configuration is viewed in the security configuration). The Bcast Key Refresh Rate and the Session Key Refresh Rate are the WPA enterprise authentication mode defaults. Click **OK**.



5.3 Configure VLAN

Type the VLAN ID in the **VLAN** box, and then bind it to the network. (The **VLAN ID** field belongs to the Network page, and when the user inputs any VLAN ID here, it automatically binds to the network currently being modified. Binding in this instance means tying a VLAN ID to a particular IP network.) This VLAN ID is the data VLAN that the client uses.

5.4 MAC authentication

Click **MAC Authentication Mode** to enable MAC authentication. MAC authentication controls the client's access to the network by configuring the black and white list (detailed in Chapter 10: WIDS security). Select the **Config Black and White List** check box.

5.5 Portal instance

Pull down the desired **Portal Instance** to enable it.

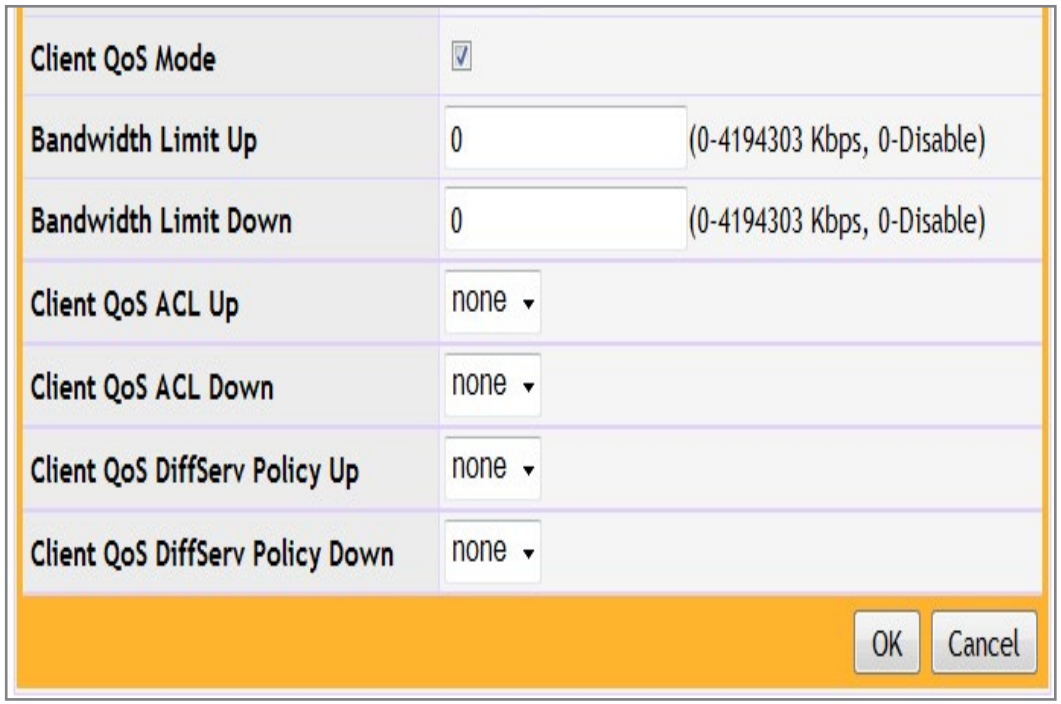
5.6 Client QoS

The Client QoS controls the client's rate and access through the network configuration.

There are three forms:

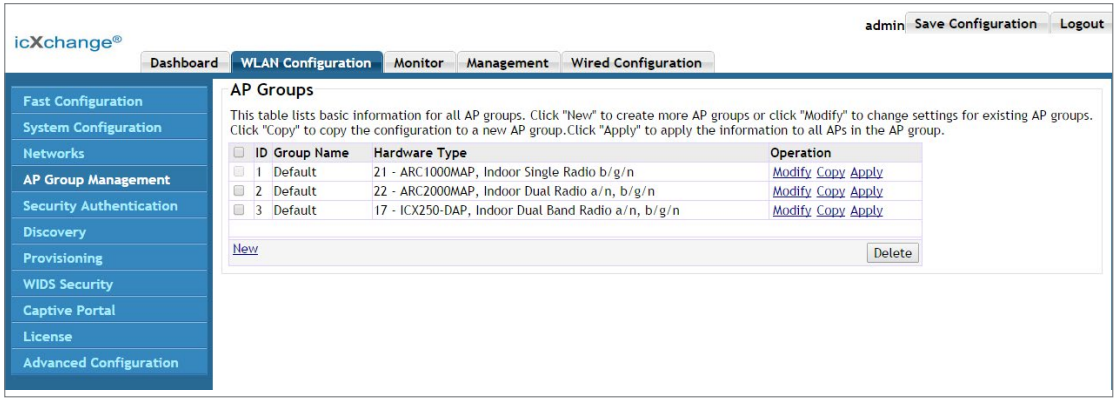
1. Client QoS bandwidth limit up and down
2. Client QoS access control up and down
3. Client QoS DiffServ policy up and down

Select the **Client-Qos Mode** check box:



Chapter 6: AP group management

AP Group MangementMRes is used to manage multiple APs. Multiple APs can be added and managed in one AP group. Click **WLAN Configuration->AP Group Management** to open into the **AP Group Management** page. The user can configure each of the AP group items and submit them to the Link1000ACS.

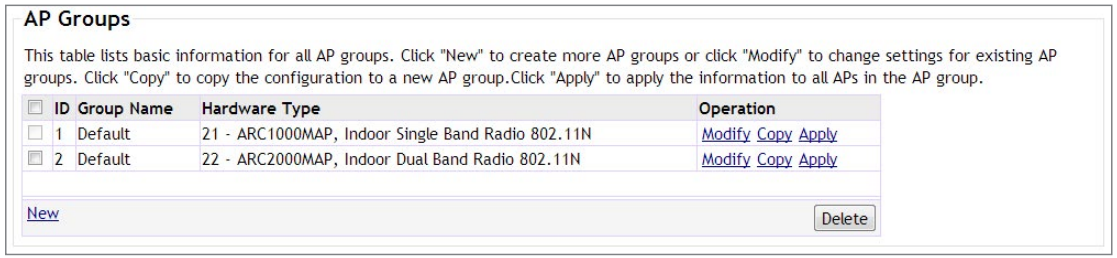

admin
Save Configuration
Logout
icXchange
Dashboard
WLAN Configuration
Monitor
Management
Wired Configuration
Fast Configuration
System Configuration
Networks
AP Group Management
Security Authentication
Discovery
Provisioning
WIDS Security
Captive Portal
License
Advanced Configuration
AP Groups
This table lists basic information for all AP groups. Click "New" to create more AP groups or click "Modify" to change settings for existing AP groups. Click "Copy" to copy the configuration to a new AP group.Click "Apply" to apply the information to all APs in the AP group.
ID Group Name Hardware Type Operation
1 Default 21 - ARC1000MAP, Indoor Single Radio b/g/n Modify Copy Apply
2 Default 22 - ARC2000MAP, Indoor Dual Radio a/n, b/g/n Modify Copy Apply
3 Default 17 - ICX250-DAP, Indoor Dual Band Radio a/n, b/g/n Modify Copy Apply
New
Delete

6.1 Add/modify/delete AP group

The **New** and **Modify** links and the **Delete** button can configure the AP groups.

Example:

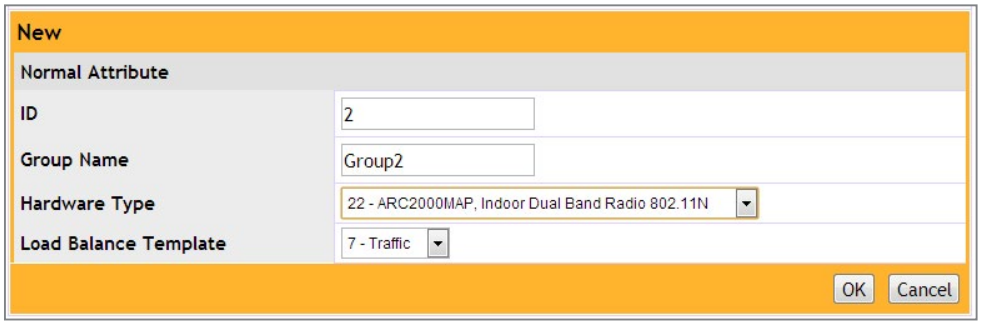
1. Click **New**, and type the ID as **2**. Click **OK**.
2. Click **Modify** to the right of AP group 2 to modify.
3. Select AP group 2, and click **Delete** to delete this AP group (AP group 1 cannot be deleted - it is used to record failed and rogue APs).


AP Groups
This table lists basic information for all AP groups. Click "New" to create more AP groups or click "Modify" to change settings for existing AP groups. Click "Copy" to copy the configuration to a new AP group.Click "Apply" to apply the information to all APs in the AP group.
ID Group Name Hardware Type Operation
1 Default 21 - ARC1000MAP, Indoor Single Band Radio 802.11N Modify Copy Apply
2 Default 22 - ARC2000MAP, Indoor Dual Band Radio 802.11N Modify Copy Apply
New
Delete

6.1.1 Normal attribute

Click **New** or **Modify** to open the AP group's **Normal Attribute** page. The user can enter the basic configuration information of the AP group from this page.

Example: Type the ID as **2** and the Group Name as **Group2**. Select the Hardware Type as **22** and the Load Balance Template as **7 – Traffic**. Click **OK**.



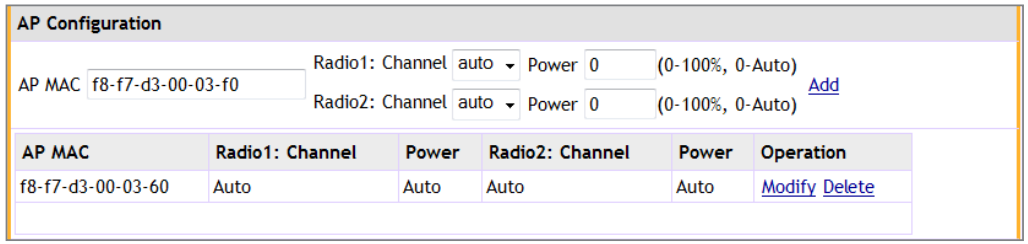
The configured hardware type should be the same as the actual AP. Hardware types include **Dual Radio (type 22)** and **Single Radio (type 21)**. The hardware type of **0** is the default value, which means that there is no corresponding AP. Details of load balance template creation can be found in Chapter 14. In this example, the load balance template is bound to Group2.

6.1.2 AP configuration

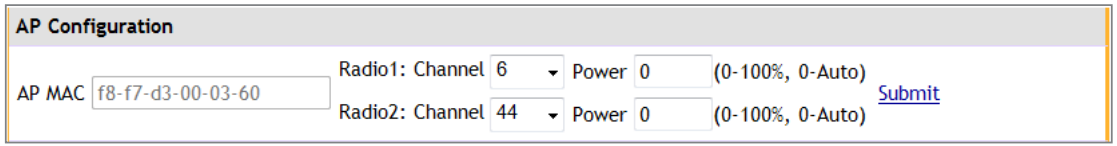
From the **AP Configuration** page, the user can add, modify, or delete the AP in the AP group and configure the channel and power. The AP can only be configured when the AP group is modified. This action takes effect immediately and is submitted to the Link1000ACS without clicking **OK** (at the bottom right of the page).

Example:

1. Type the AP MAC address in the AP MAC box as **f8-f7-d3-00-03-f0**. Select the Channel as **auto**. Type the Power as **0** (0 power indicates automatic power adjustment). Click **Add**.



2. Click **Modify** to the right of the AP to modify it. The AP MAC address cannot be modified, but the channels and power can be. Select the Channel to be **6** and the Power to be **0**. Click **Submit.**

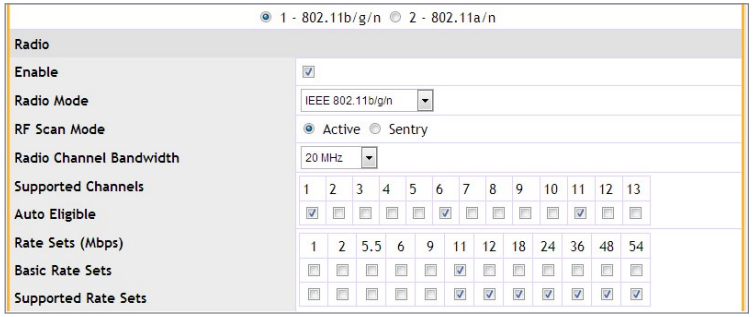


3. Click **Delete** to the right of the AP that needs to be deleted. When deleting an AP from a group, you must reset the AP. Click the **Monitor** tab, click **AP**, click **View Detail** and then pull down the radio mac address to reset in **Managed AP Status**. Scroll down the page to click the **Reset** button. The AP will reset in about 2 minutes.

6.1.3 Radio

The Radio section configures the radio of the AP group. The Radio, VAP, QoS, and TSPEC are all configured in one radio. Select the hardware type button on an AP that has dual radios. The radio, which needs to be configured, can be selected here. Switching the radio will cause any unsaved changes to be lost. Submit changes before switching the radio.

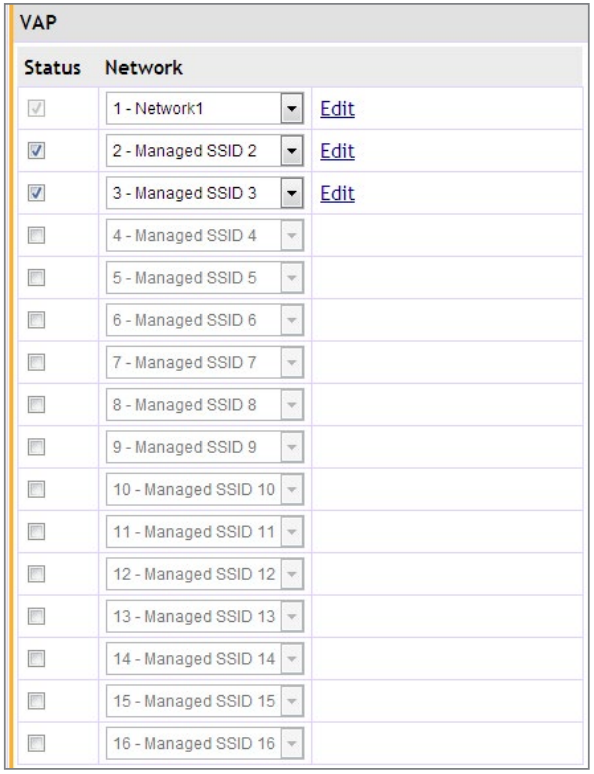
Example: Select the **Enable** check box, and then select the Radio Mode as **IEEE 802.11b/g/n**. Select the RF Scan Mode as **Active**, the Radio Channel Bandwidth as **20 MHz**, the supported radio rates, and select the check box for the eligible radio channels. Click **OK** to generate the created or modified AP group.



- Radio Mode: the user can select **IEEE 802.11b/g/n**, **IEEE 802.11b/g**, **2.4GHz IEEE 802.11n**, **IEEE802.11b**, or **IEEE 802.11g** in radio 1. The user can select **IEEE 802.11a/n**, **IEEE 802.11a**, or **5GHz IEEE 802.11n** in radio 2.
- RF Scan Mode: includes **Active** and **Sentry** modes.
- Radio Channel Bandwidth: includes three modes (**20MHz**, **40MHz**, and **20/40MHz** can be selected).
- Auto Eligible: shows the channels that the AP can choose when implementing auto channel adjustment.
- Rate Sets (Mbps): the user can select the basic and supported rates through the check boxes.

6.1.4 VAP

VAP configures the networks used by all APs in the AP group. Select the **Status** check box next to the VAP that needs to be enabled, and then select the network name. Click **Edit** to configure the network (detailed in Chapter 5: Networks). Click **OK**.

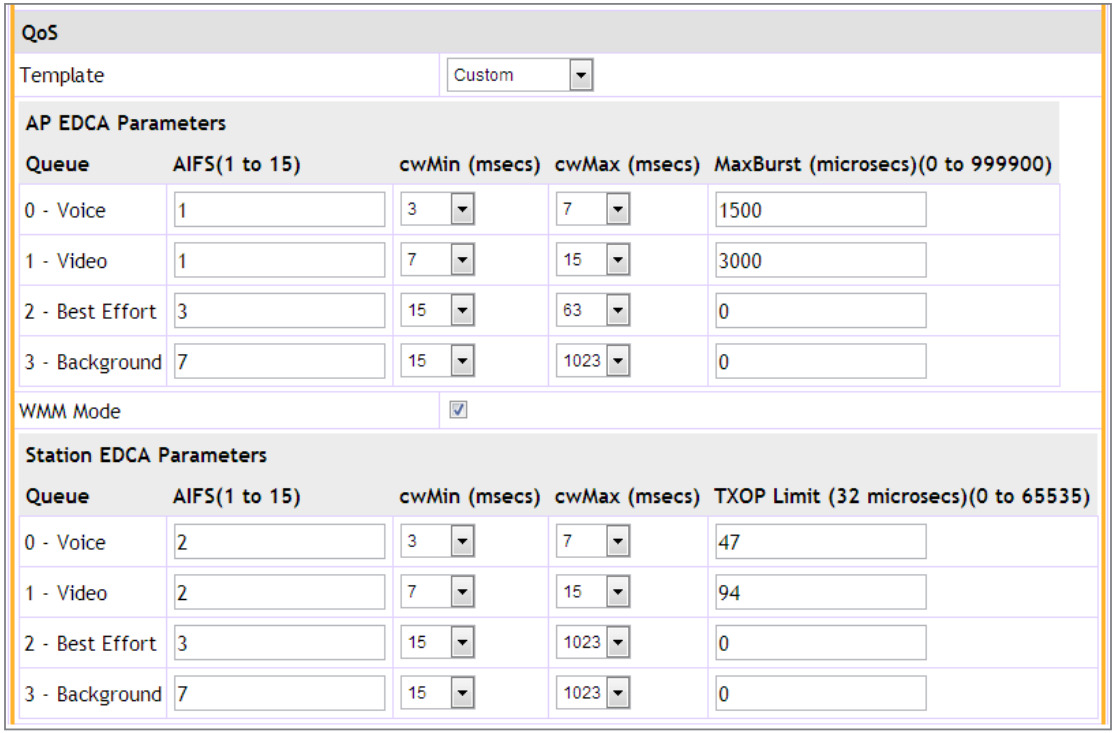


VAP: Abbreviation for Virtual Access Point. VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple APs in one physical AP. You can configure up to 16 VAPs for each radio, and they correspond to networks 1-16.

6.1.5 QoS

Custom QoS policies and rules can be created in the QoS section of the WebGUI. For optimal user experience, all key fields are configured by default.

Example: Select the Template as **Custom**. Select the **WMM Mode** check box. Each of the EDCA parameters are configured as the default value. Click **OK**.

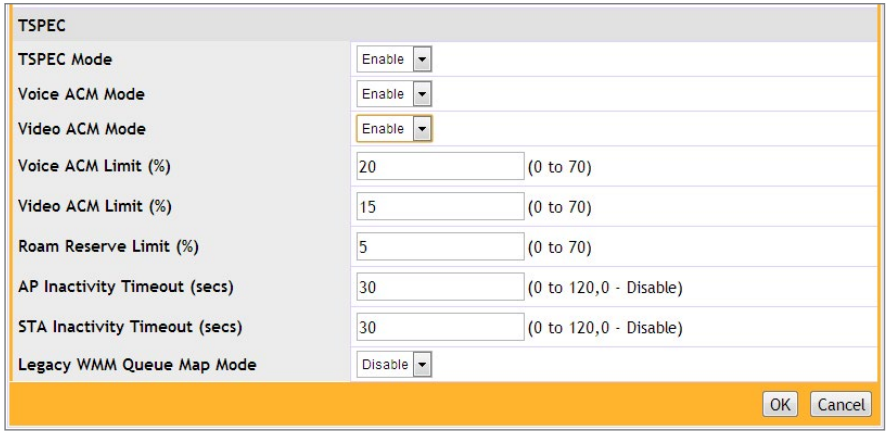


- Template: The user can select **Custom, Factory Default**, or **Voice**. EDCA parameters can only be configured when **Custom** is selected.
- AP EDCA Parameters: The user can type values or select from the drop-down lists to configure AP EDCA parameters.
- WMM Mode: The user can select or clear the check box to enable or disable the WMM QoS function.
- Station EDCA Parameters: The user can type values or select from the drop-down lists to configure EDCA parameters.

6.1.6 TSPEC

Traffic Specifications (TSPEC) parameters can be configured here for the AP group or groups. Generally, the configured default values are appropriate for most users. Only advanced users should configure these parameters.

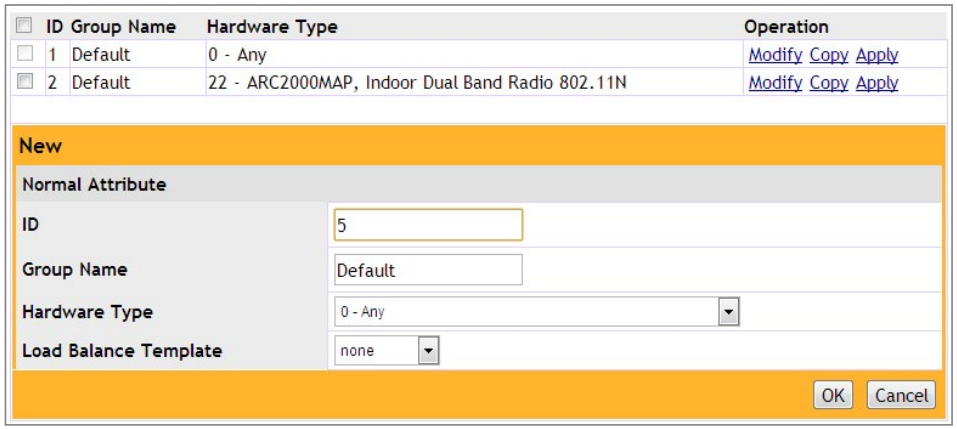
Example: Select **Enable** for the TSPEC Mode. Select **Enable** for the Voice ACM Mode and Video ACM Mode. Type the limit and timeout as the default values, and click **OK**.



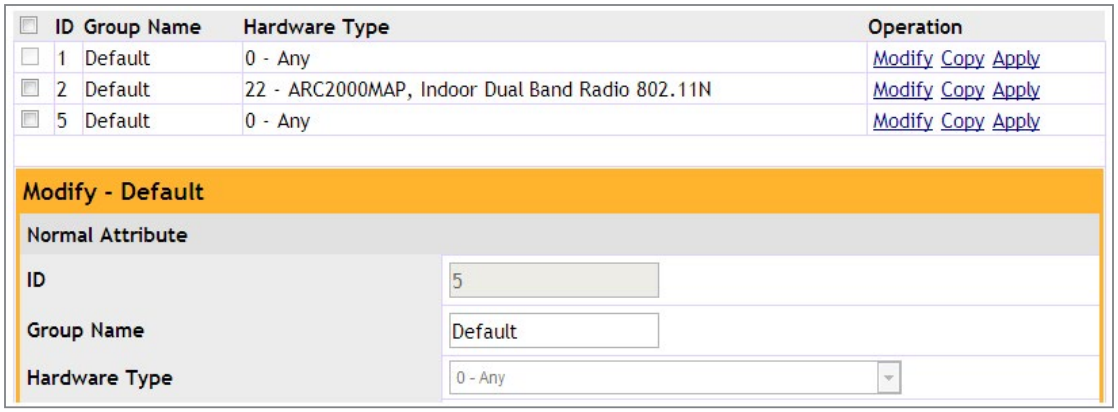
6.2 Copy AP group

Copying allows users to quickly create or modify new AP groups.

Example: Click **New** to create the AP group. Type the ID as **5**, and then click **Copy** to the right of AP group 1. AP group 5 will be created, and its configuration will be the same as AP group 1. AP MAC addresses will not be copied during this process.



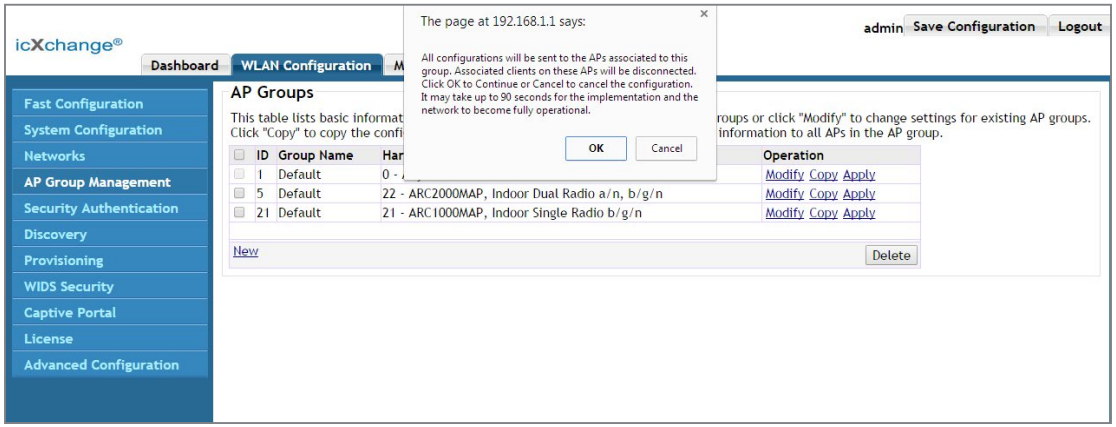
1. Click **Modify** to the right of AP group 5 to modify it. Click **Copy** to the right of AP group 2. AP group 5 will be modified, and its configuration will be the same as AP group 2.


ID Group Name Hardware Type Operation
1 Default 0 - Any Modify Copy Apply
2 Default 22 - ARC2000MAP, Indoor Dual Band Radio 802.11N Modify Copy Apply
5 Default 0 - Any Modify Copy Apply
Modify - Default
Normal Attribute
ID 5
Group Name Default
Hardware Type 0 - Any

6.3 Apply AP group

Click **Apply** to the right of the AP group to send the configuration to the APs. After configuring the AP group, click **OK**. Configurations will be pushed to that group within about 90 seconds.

Example: Click **Apply** to the right of AP group 5, and then click **OK** to send the configuration to all the APs in AP group 5.


icXchange
admin Save Configuration Logout
Dashboard WLAN Configuration
Fast Configuration
System Configuration
Networks
AP Group Management
Security Authentication
Discovery
Provisioning
WIDS Security
Captive Portal
License
Advanced Configuration
AP Groups
The page at 192.168.1.1 says:
All configurations will be sent to the APs associated to this group. Associated clients on these APs will be disconnected. Click OK to Continue or Cancel to cancel the configuration. It may take up to 90 seconds for the implementation and the network to become fully operational.
OK Cancel
ID Group Name Operation
1 Default Modify Copy Apply
5 Default 22 - ARC2000MAP, Indoor Dual Radio a/n, b/g/n Modify Copy Apply
21 Default 21 - ARC1000MAP, Indoor Single Radio b/g/n Modify Copy Apply
New
Delete

Chapter 7: Security authentication

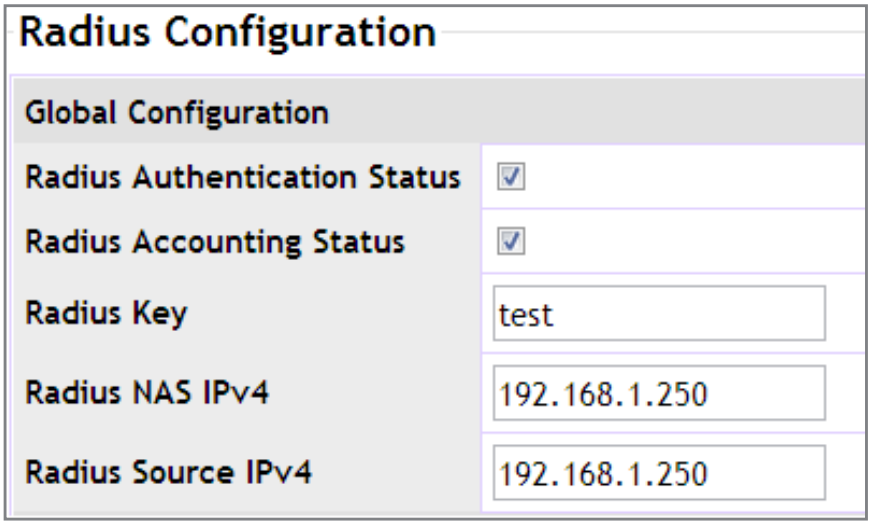
The **Security Authentication** module includes Radius and LDAP configuration. Radius configuration includes **Global Configuration, Radius Authentication Server Configuration, Radius Accounting Server Configuration, Radius Group Manage**, and **Radius Configuration**.

7.1 Radius configuration

7.1.1 Global configuration

Prior to enabling the Radius authentication and accounting service, configure an accounting server and an authentication server. (The server configuration is covered in Section 7.1.2) After configuring the accounting and authentication servers, select the **Radius Authentication Status** check box to enable the Radius function. This corresponds to the **aaa enable** command. Select the **Radius Accounting Status** check box to enable the Radius accounting function. This corresponds to the **aaa-accounting enable** command. In the Radius Key text box, type **test** (or the secret key programmed in the radius server). This corresponds to the **radius-server key** command. The key must be the same as the Radius server for authentication.

Type the address as **192.168.1.250** for both the Radius NAS IPV4 and Radius Source IPV4 boxes. The configuration of NAS IP corresponds to the **radius nas-ipv4** command. The Radius Source IPV4 corresponds to the **radius source-ipv4** command.



After all fields are entered, click **Submit**.

7.1.2 Radius authentication server configuration

Radius Authentication Configuration corresponds to the **radius-server authentication host** command and can configure the address of the authentication server.

Example: Configure the Server IP Address as **192.168.1.15**. Select the **Primary Authentication Server** check box, as shown in the following figure:

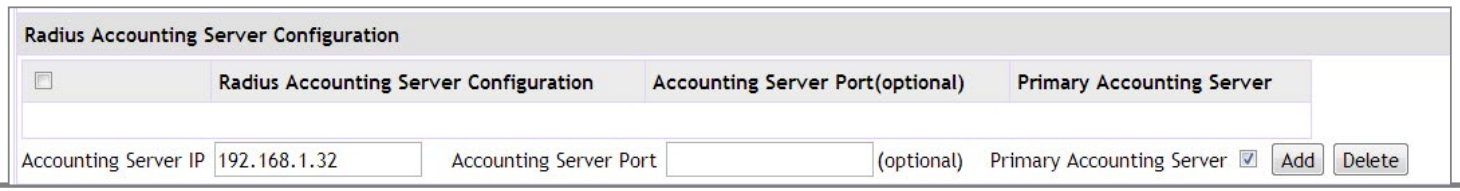
Click **Add**.

The default Authentication Server Port is **1812**. To delete the server, select it, and then click **Delete**. Prior to deleting the last authentication server, the **Radius Authentication Server** must be disabled. Click **Submit** to save the configuration.

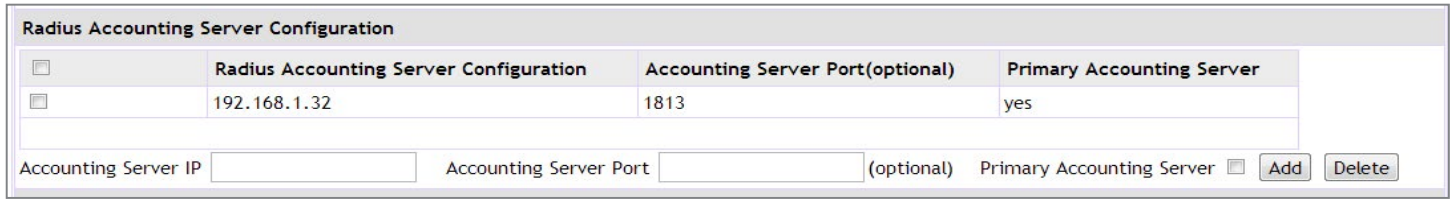
7.1.3 Radius accounting server configuration

Radius Accounting Configuration corresponds to the **radius-server accounting host** command and can configure the accounting server's address.

Example: Configure the Accounting Server IP as **192.168.1.32**. If the Authentication Server Port field is empty, the value is set to the default value. Select the **Primary Accounting Server** check box, as shown in the following figure:



Click **Add**.

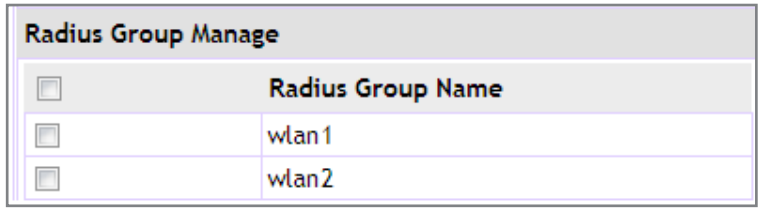


The default Accounting Server Port is 1813. If deleting the accounting server, select it, and then click **Delete**. Prior to deleting the last accounting server, the Radius Accounting Server must be disabled. Click **Submit** to save the configuration.

7.1.4 Radius group manage

Radius Group Manage corresponds to the **aaa group server radius** command. It can configure multiple Radius groups.

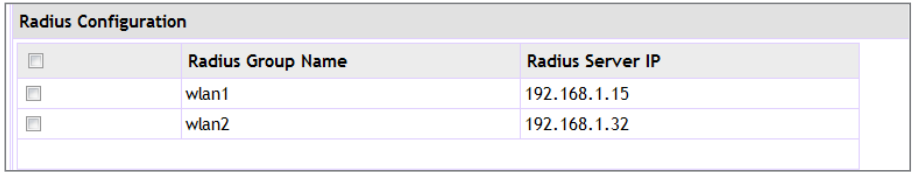
Example: Configure two Radius groups of wlan1 and wlan2. Type the group names in the Radius Group Name text box, and then click **Add**.



7.1.5 Radius configuration

Radius Configuration will bind the Radius server address to the Radius group. Multiple Radius addresses can be bound to each group name, but each Radius address can only be bound to one Radius group.

Example: Bind the 192.168.1.15 server to wlan1, and bind the 192.168.1.32 server to wlan2. Choose the configured Radius group in the Radius Group Names, and select the server address in the **Radius Server IP** drop-down list. Click **Add**.



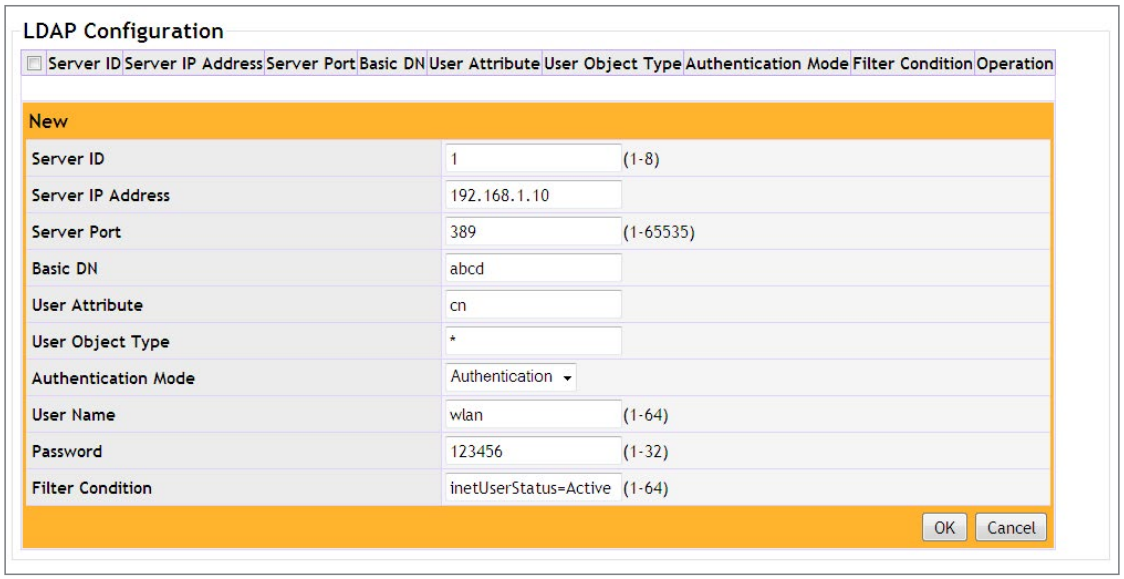
After configuring, click **Submit** to save the configuration.

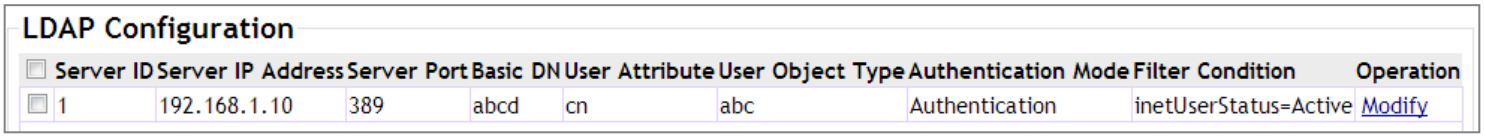
7.2 LDAP configuration

LDAP Configuration corresponds to the **ldap server + subsequent configuration** command and is mainly used by the portal authentication server and user management server. The main configuration items include the following:

- Server IP Address: the LDAP server IP address.
- Server Port: LDAP server port (default port is 389).
- Basic DN: base DN that the user wants to find for the LDAP server.
- User Attribute: user attribute on the LDAP server.
- User Object Type: type of the LDAP server.
- Authentication Mode: simple and anonymous authentication (simple authentication requires user name and password).
- User Name: the appointed username.
- Password: the appointed password.
- Filter Condition: additional condition for configuring required by the user.

Example: Configure the LDAP server 1. Type the Server IP Address as **192.168.1.10**, the Server Port as **389**, Basic DN as **abcd**, the User Attribute as **cn**, and the User Object Type as **abcd**. Select the Authentication Mode as **Authentication**, the User Name as **wlan**, the Password as **123456**, and the Filter Condition as **inetUserStatus=Active**. Click **OK.**





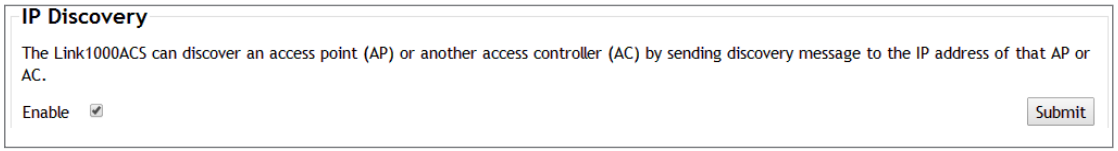
After configuring, select **Modify** to modify the configured LDAP server. The user can also delete the configured LDAP server by clicking **Delete**.

Chapter 8: Discovery

8.1 IP discovery

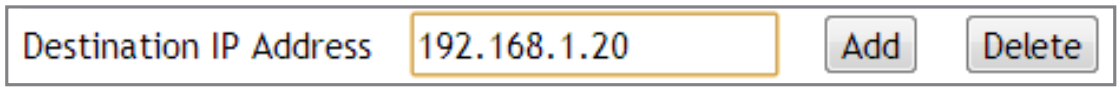
8.1.1 Enable and disable IP discovery

Click **WLAN Configuration->Discovery->L3/IP Discovery**, select **Enable**, and then click **Submit**. This enables the L3 discovery. If the check box is not selected, the L3 discovery will be disabled.


IP Discovery
The Link1000ACS can discover an access point (AP) or another access controller (AC) by sending discovery message to the IP address of that AP or AC.
Enable
Submit

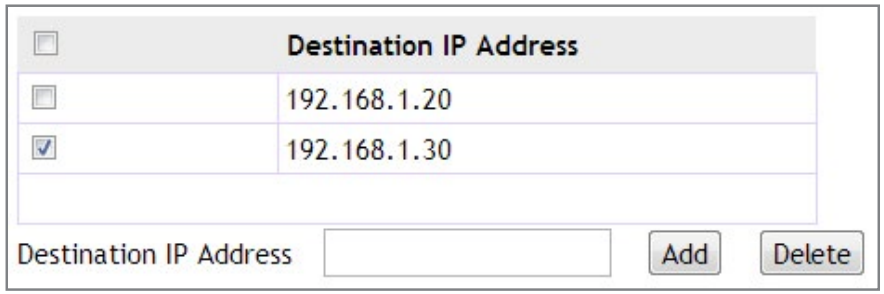
8.1.2 Add IP of L3/IP discovery

Type the IP address in the Destination IP Address box, and then click **Add** to add it into the discovery list.



8.1.3 Delete IP address from L3/IP discovery list

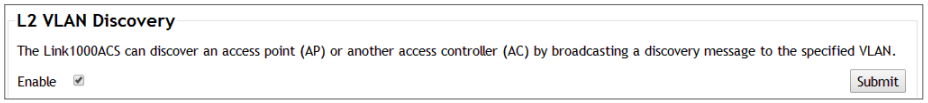
Select the IP address that needs to be deleted, and then click **Delete**. The selected IP address will be deleted.



8.2 L2 VLAN discovery

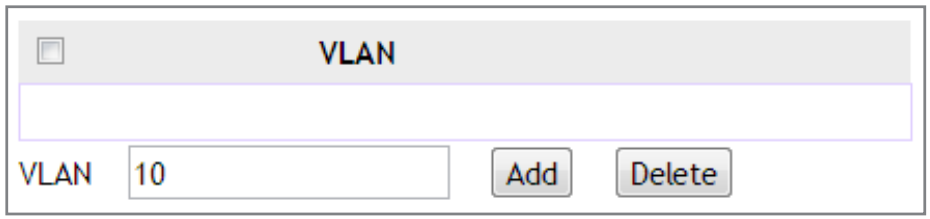
8.2.1 Enable L2 VLAN discovery

Click **WLAN Configuration->Discovery->L2/VLAN Discovery**, and then select **Enable**. Click **Submit** to enable L2 discovery.


L2 VLAN Discovery
The Link1000ACS can discover an access point (AP) or another access controller (AC) by broadcasting a discovery message to the specified VLAN.
Enable
Submit

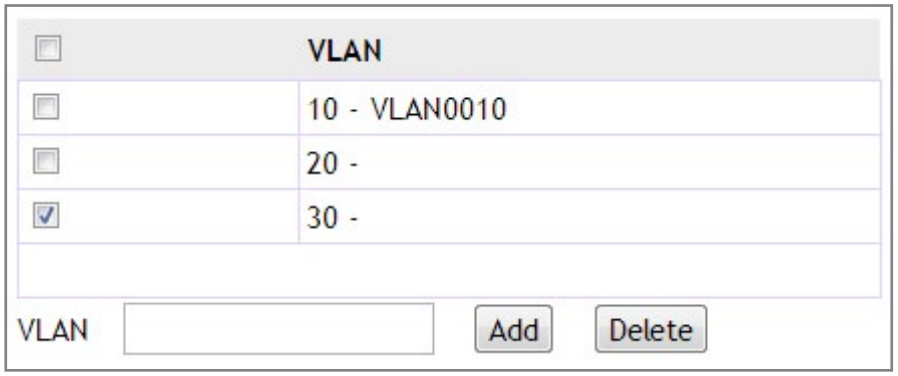
8.2.2 Add VLAN of L2/VLAN discovery

Type the VLAN in the VLAN text box, and then click **Add** to add it into the discovery list.



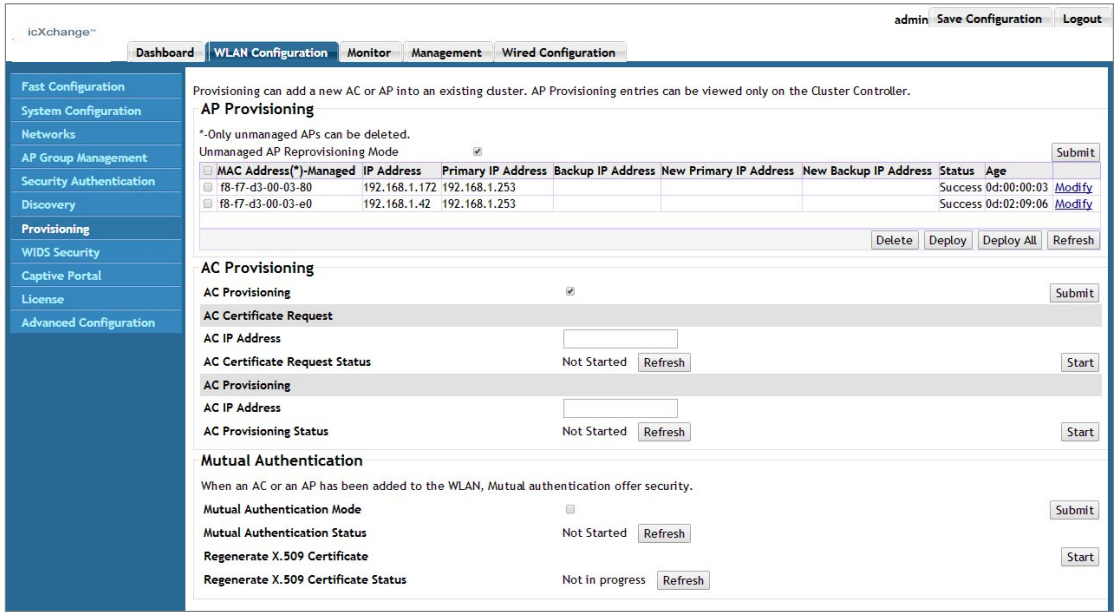
8.2.3 Delete VLAN from L2 VLAN discovery list

Select the VLAN that needs to be deleted, and then click **Delete**. The VLAN will be deleted.



Chapter 9: Provisioning

Click **WLAN Configuration->Provisioning** to open the **Provisioning** page, which will configure the AP and the Link1000ACS.



9.1 AP provisioning

AP Provisioning configures the AP for provisioning through the Link1000ACS Access Control Switch. It will provision an AP that was added into the cluster, and also provision an AP that is not added to the cluster (AP reprovisioning). Configure the Link1000ACS Access Control Switch to provision the AP. The certificate needed to authenticate will be transmitted in the cluster automatically, which will allow provisioning to begin.

Example: Click **Modify**, and type the new Primary IP Address and the new Backup IP Address of the controller to which the AP will be provisioned. Click **Submit**. Select the AP that needs provisioning, and then click **Deploy** to provision successfully.

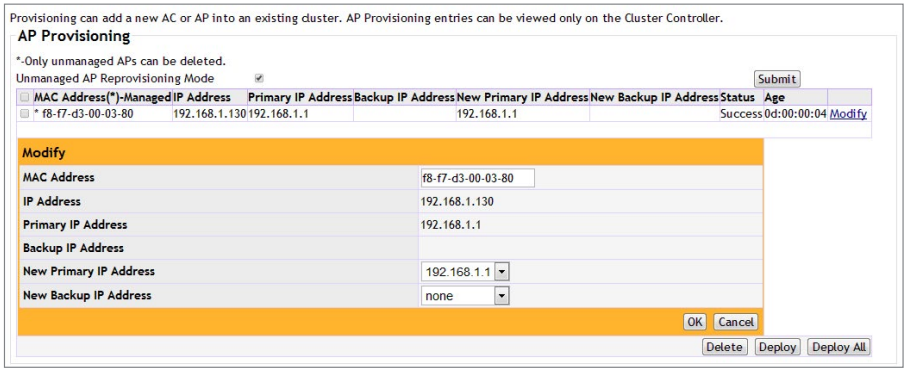
Note: The AP needs to be rebooted for a successful provision. Power down the AP manually, or if the AP has been previously managed, click the **Monitor** tab, click **AP**, click **View Detail** and then pull down the radio mac address to reset in **Managed AP Status**. Scroll down the page to click the **Reset** button. The AP will reset in about 2 minutes.

9.2 AC provisioning

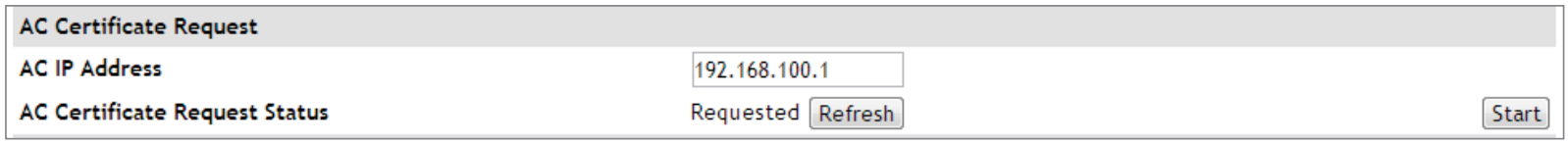
AC Provisioning adds the Link1000ACS into the cluster. This Link1000ACS needs to obtain the certificates of all ACs in the cluster. Every Link1000ACS in the cluster needs to obtain the certificate of that AC. Any Link1000ACS in the cluster can achieve the certificate transit among the Link1000ACSs.

Example:

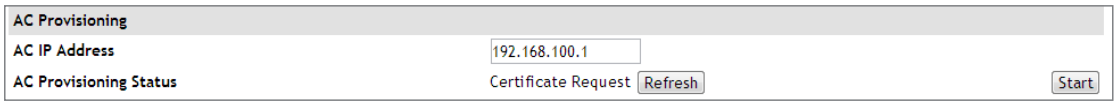
1. Select **AC Provisioning**, and click **Submit** to enable this function.



2. Type **192.168.100.1** (the IP address of the Link1000ACS to be added to the cluster) in the AC IP Address text box , and click **Start**. The certificate request will begin. Click **Refresh** to view the status.



3. Type **192.168.100.1** (the IP address of the Link1000ACS to be added to the cluster) in the AC IP Address text box, and click **Start**. The provisioning will begin. Click **Refresh** to view the status.

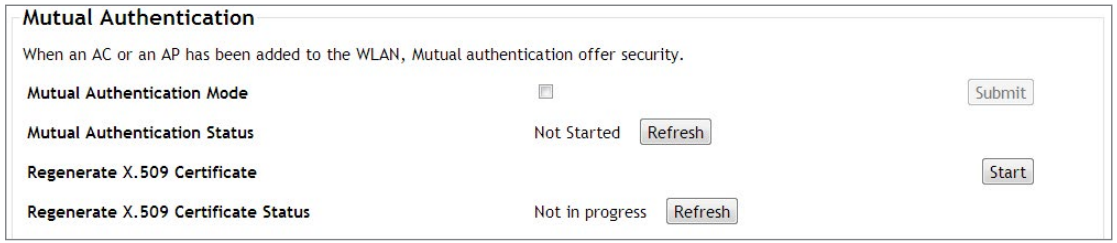


9.3 Mutual authentication

Mutual Authentication can be enabled to avoid the risk of an unknown device joining the cluster. This function allows only devices with a certificate to pass authentication and join the cluster by issuing the X.509 certificate.

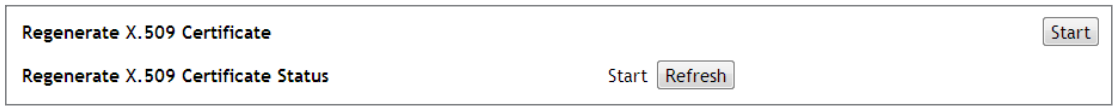
Example:

1. Select the **Mutual Authentication Mode** check box, and then click **Submit** to enable this mode. Click **Refresh** to view the status of the last network mutual authentication.



2. Click **Start** to regenerate the X.509 certificate. Click **Refresh** to view the process of the Link1000ACS authentication regeneration.

Note: The certificate is only produced once; the status will revert to **Not Started** after being produced.

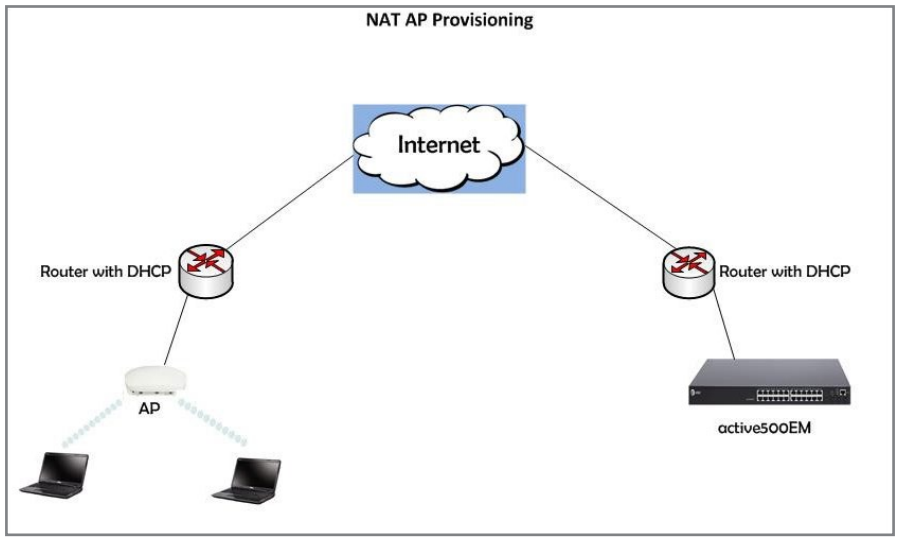


Chapter 10: Provisioning over NAT

The icXchange® solution can be deployed over a NAT environment. NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. This allows users to utilize the icXchange® access point products in remote office environments for enterprise deployments, and in multi-client environments for managed service provider deployments. For example, the Link1000ACS can be located in the one central location or Network Operations Center and communicate with icXchange® access points in remote locations. The icXchange® solution essentially virtualizes the Internet cloud as a direct link to devices.

The Link1000ACS can support up to 132 icXchange® access points over NAT configurations and each icXchange® access point has the capability to configure up to three Link1000ACS controllers as backups for redundancy in case the master controller is inaccessible for any reason.

The NAT AP Provisioning diagram below displays a typical network topological layout of an access point provisioning over a NAT based environment. Here, both the icXchange® access points and the Link1000ACS controller are both behind NAT based firewalls utilizing private IP addresses.



10.1 NAT provisioning configuration

Both the icXchange® APs and the Link1000ACS access controller must be configured to complete the NAT configuration.

10.1.1 NAT ports

The Link1000ACS and associated access points use TCP ports 57776-57779 to communicate over NAT. Set a policy on your NAT firewalls, gateways, and/or routers to open TCP ports 57776-57779 to all associated icXchange® devices on the local and remote networks. Please refer to the NAT device/firewall manufacturer's user documentation for proper configuration.

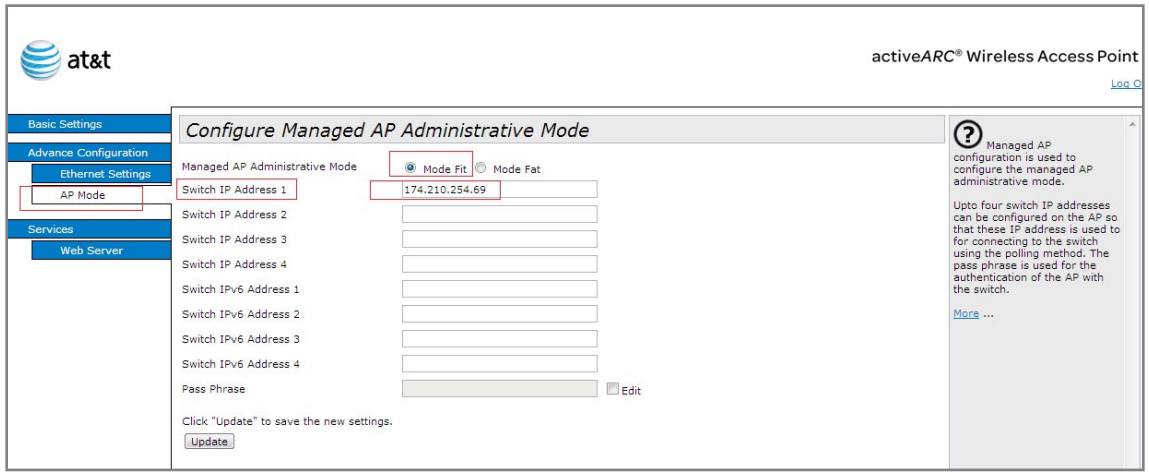
10.1.2 Access point NAT configuration

Configure the icXchange® Access Point in Fit mode by selecting Advanced Configuration > AP Mode and choosing Mode Fit.

Under **Configure Managed AP Administrative Mode**, enter the global/public IP address of the NAT supporting firewall, gateway, and/or router, which is front of the Link1000ACS Access Controller (e.g. 174.210.254.69), in the **Switch IP Address 1** field. Click **Update**.

If the Link1000ACS Access Controller is not set up behind a NAT supporting gateway and is placed directly on a public IP address, then that public IP address would be entered in the **Switch IP Address 1** field.

Up to three additional Link1000ACS Access Controller IP addresses can be entered in the fields **Switch IP Address 2**, **Switch IP Address 3,** and **Switch IP Address 4** as backups.


at&t
activeARC® Wireless Access Point
Log O
Basic Settings
Advance Configuration
Ethernet Settings
AP Mode
Services
Web Server
Configure Managed AP Administrative Mode
Managed AP Administrative Mode
Mode Fit
Mode Fat
Switch IP Address 1
174.210.254.69
Switch IP Address 2
Switch IP Address 3
Switch IP Address 4
Switch IPv6 Address 1
Switch IPv6 Address 2
Switch IPv6 Address 3
Switch IPv6 Address 4
Pass Phrase
Edit
Click "Update" to save the new settings.
Update
Managed AP configuration is used to configure the managed AP administrative mode.
Upto four switch IP addresses can be configured on the AP so that these IP address is used to for connecting to the switch using the polling method. The pass phrase is used for the authentication of the AP with the switch.
More ...

10.2 Link1000ACS access controller NAT configuration

10.2.1 NAT ports

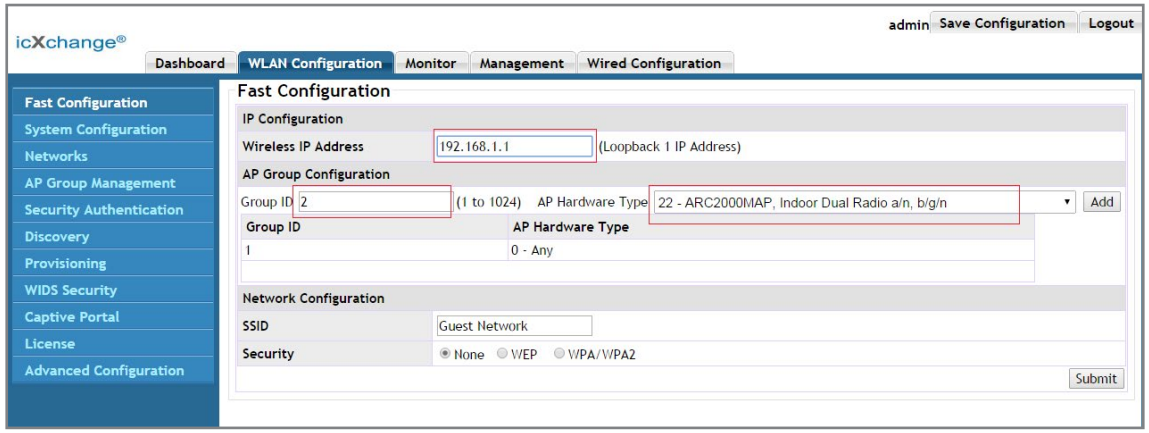
The Link1000ACS and associated access points use TCP ports 57776-57779 to communicate over NAT. Set a policy on your NAT firewalls, gateways and/or routers to open TCP ports 57776-57779 to all associated icXchange® devices on the local and remote networks. Configuration for opening these ports would depend upon the type and the brand of the NAT device used, and how that NAT device allows certain ports to be opened. Please refer to the NAT firewall, gateway and/or Virtual Server manufacturer's user documentation for proper configuration.

If a public IP address is used for the Link1000ACS's default controller IP address, it is not necessary to perform the port opening configuration. There is no NAT firewall, gateway and/or Virtual Server present between the Link1000ACS and the Internet if a public IP address is set as the default.

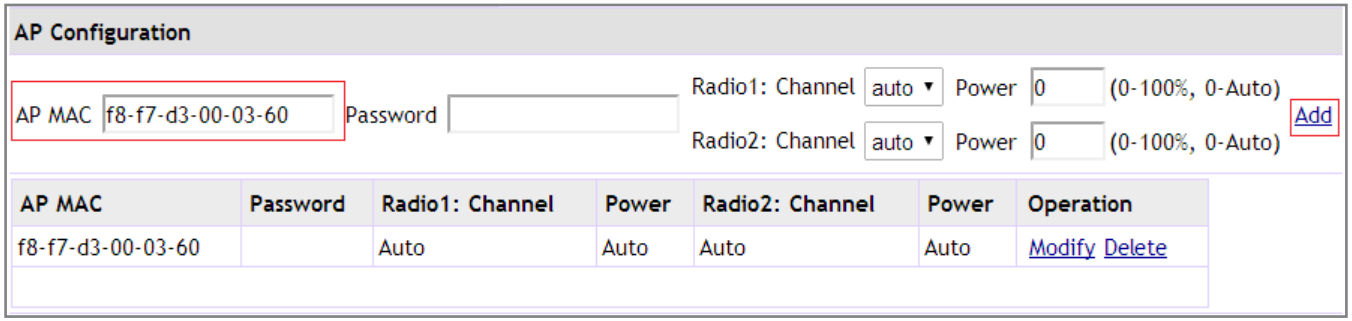
10.2.2 Link1000ACS NAT configuration

Click **WLAN Configuration > Fast Configuration**. Enter the default VLAN IP address for the actve500EM in the field Wireless IP Address. The default IP address for the Link1000ACS is **192.168.1.1** if it has not been updated in prior configurations.

1. Type **1** in the Group ID field, and from the AP Hardware Type dropdown select **22** for the *ARC*2000MAP and *ARC*3000MAP Dual Band Access Points, or **21** for the *ARC*1000MAP Single Band Access Point. Click **Add** to add the AP Group configuration. Click **Submit** to save the configuration.



2. Select **WLAN configuration >AP Group Management**. Click **Modify** on the group created in the previous step.
3. Enter the AP's MAC address, for example, **f8-f7-d3-00-03-60** and click **Add**. Click **OK**.

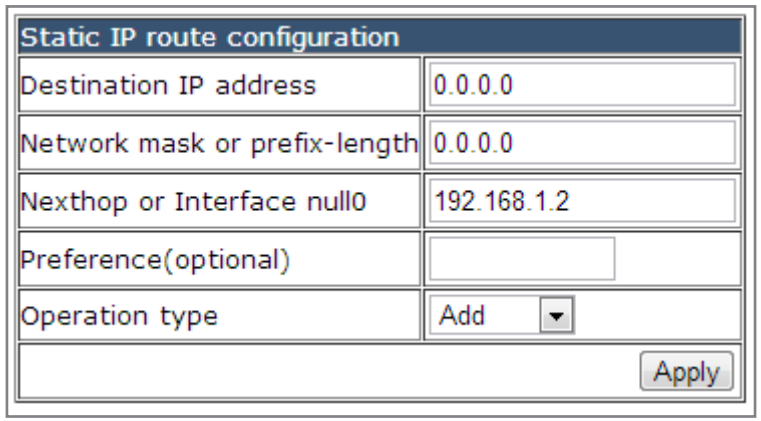

AP Configuration
AP MAC f8-f7-d3-00-03-60
Password
Radio1: Channel auto Power 0 (0-100%, 0-Auto)
Radio2: Channel auto Power 0 (0-100%, 0-Auto)
Add
AP MAC Password Radio1: Channel Power Radio2: Channel Power Operation
f8-f7-d3-00-03-60 Auto Auto Auto Auto Modify Delete

4. Select **Provisioning** from the left navigation bar to check the AP Provisioning status.

A static route may need to be created for the traffic to flow correctly across the NAT setup. Click **Wired Configuration** > **Route Configuration> Static route configuration**.

Example: In this example the next hop IP address 192.168.1.2 is used based on the controller IP address of 192.168.1.1.

Type **0.0.0.0** in the Destination IP address field**, 0.0.0.0** in the Network mask or prefix-length field, and **192.168.1.2** in the Nexthop or Interface null0 field. Select Operation type **Add** and click **Apply**.

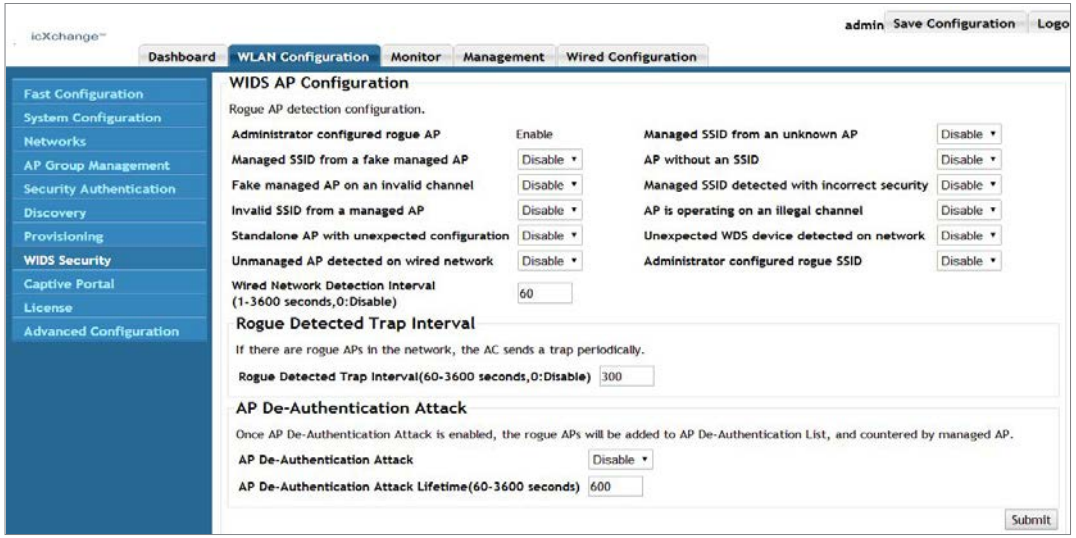


The AP will provision within 90 seconds. The status of the AP can be viewed in the Dashboard, or on the Provisioning page.

Click **Save Configuration** on the top of the page to save your configurations on the Link1000ACS.

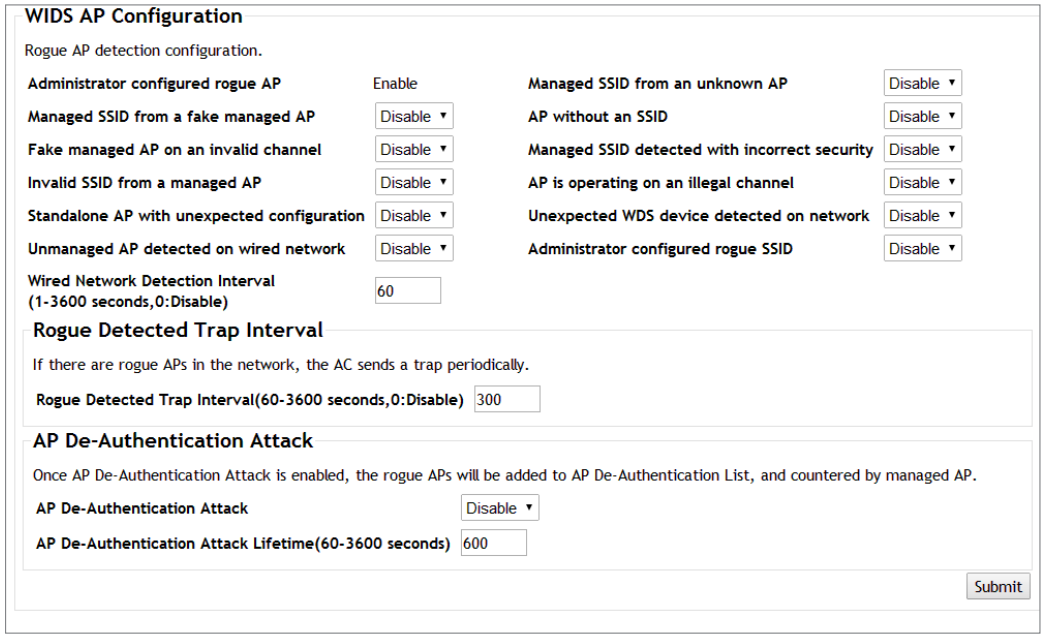
Chapter 11: WIDS security

Click **WLAN Configuration->WIDS Security** to open the **WIDS Security** page, which includes three modules: **WIDS AP Configuration**, **WIDS Client Configuration**, and **Known Client**. Every module occupies one rectangular box , and they can be used to configure the WIDS AP configuration, WIDS client configuration, and black and white list.



11.1 WIDS AP configuration

Click **WLAN Configuration->WIDS Security->WIDS AP Configuration** to select **Enable** or **Disable** for each item option, as shown in the following figure:

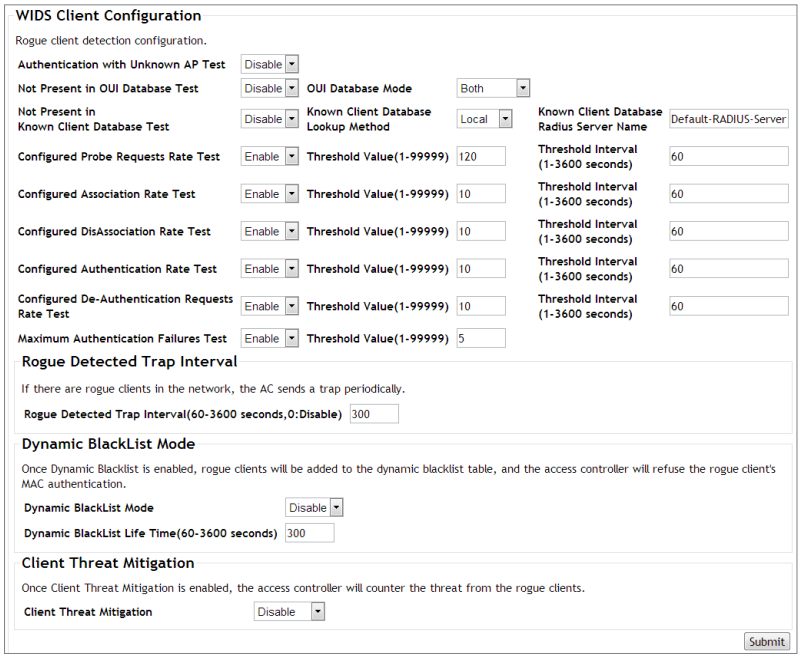


- Administrator configured rogue AP – enables the rogue AP detection configured by the administrator.
- Managed SSID from a fake managed AP – enables or disables the illegal vendor file detection in Beacon frame.
- Fake managed AP on an invalid channel – enables or disables detection of the managed AP's Beacon frame received from the invalid channel.
- Invalid SSID from a managed AP – enables or disables detection of managed APs sending an invalid SSID .
- Stand-alone AP with unexpected configuration – enables or disables the detection of stand-alone AP with unexpected configuration.
- Unmanaged AP detected on wired network – enables or disables detection of unmanaged AP accessing the wired network.
- Wired Network Detection interval (seconds) – configures the shortest waiting interval of every detection; default value is 60s.
- Managed SSID from an unknown AP – enables or disables detection of illegal AP imitating lawful SSID.
- AP without an SSID – enables or disables detection that no SSID field in Beacon frame.

- Managed SSID detected with incorrect security – enables or disables detection of AP using the incorrect security authentication mode.
- AP is operating on an illegal channel – enables or disables the detection of the managed AP Beacon from receiving on the illegal channel.
- Unexpected WDS device detected on network – enables or disables detection of unexpected WDS device based on OUI database.
- Administrator configured rogue SSID - enables the rogue SSID detection configured by the administrator.
- Rogue Detected Trap Interval (seconds) – default value is 300s.
- AP De-Authentication Attack – enables or disables the rogue AP mitigation function.
- AP De-Authentication Attack Lifetime (seconds) – configures the AP de-authentication attack lifetime; default value is 600s

11.2 WIDS client configuration

Click **WLAN Configuration->WIDS Security->WIDS Client Configuration** to configure. This enables the WIDS client detection and configures the items' parameters.

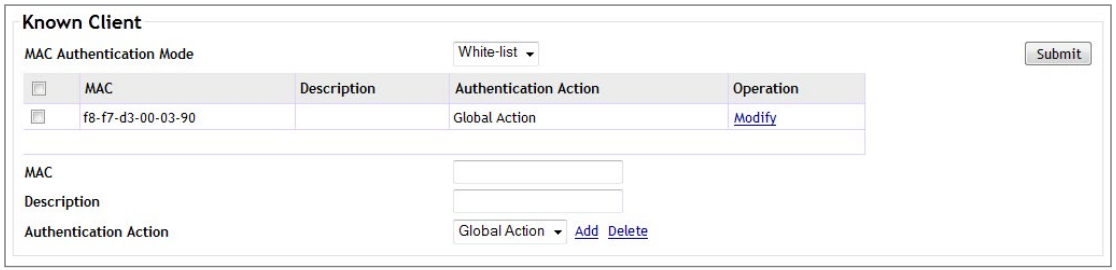


- Authentication with Unknown AP Test – enables or disables the detection of lawful client associating with an unknown AP.
- Not Present in OUI Database Test – enables or disables the OUI detection.
- OUI Database Mode – Identifies OUI database mode.
- Not Present in Known Client Database Test – enables or disables the detection of a known client.
- Known Client Database Lookup Method – configures the method of the known client database lookup; it includes two methods: local and radius.
- Known Client Database Radius Server name – configures the method of the known client database server name.
- Configured Probe Requests Rate Test – enables or disables the probe requests frame flood attacks detection.
- Configured Association Rate Test – enables or disables the association requests frame flood attacks detection.
- Configured Disassociation Rate Test – enables or disables the disassociation requests frame flood attacks detection.

- Configured Authentication Rate Test – enables or disables authentication requests frame flood attacks detection.
- Configured De-Authentication Requests Rate Test – enables or disables the de-authentication requests frame flood attacks detection.
- Maximum Authentication Failures Test – enables or disables detection of the maximum failed authentications.
- Rogue Detected Trap Interval – identifies the periodic rate that the AC sends a trap to detect rogue clients in the network.
- Dynamic Blacklist Mode – enables or disables the dynamic blacklist function.
- Dynamic Blacklist Life time – identifies the length of time for the dynamic blacklist.
- Client Threat Mitigation – enables or disables the known client protection function.

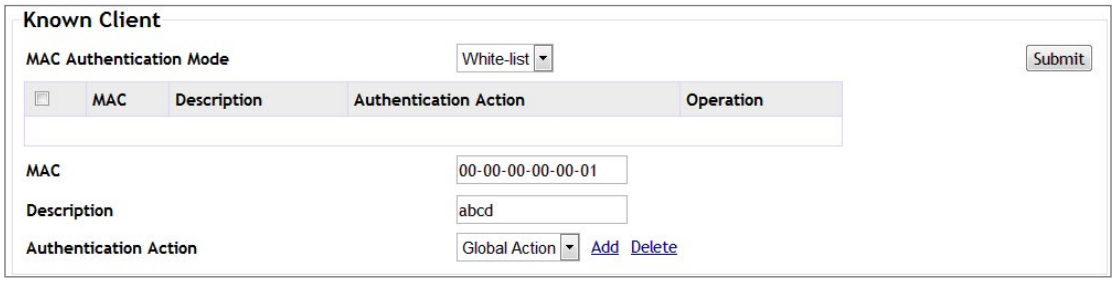
11.3 Known client

Open the **Known Client** configuration page to configure the MAC authentication mode and add, delete, or modify the black and white list.



11.3.1 MAC authentication mode

Enter into the **Known Client->MAC Authentication Mode** to choose the white or black list as the MAC authentication mode of known client.



Select the MAC Authentication Mode as **Black-list**, and then click **Submit**.

Select the MAC Authentication Mode as **White-list**, and then click **Submit**.

11.3.2 Black/white list configuration

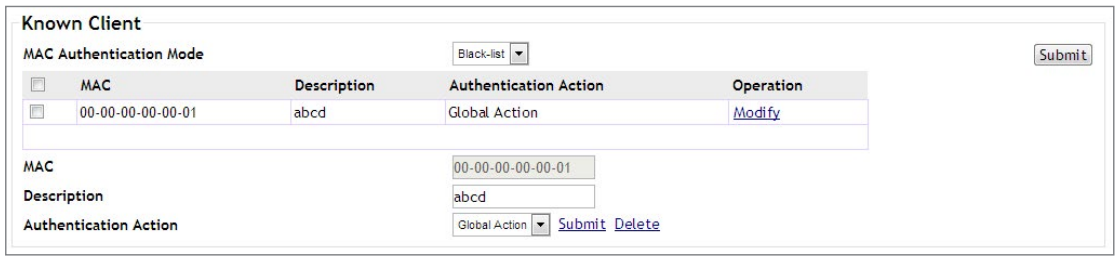
Go to the **black/white list configuration** section under the **Known Client** module to type the client MAC, Description, and Authentication Action, and then click **Add**.

- MAC – client MAC.
- Description – client description information.
- Authentication action – includes **Global Action**, **Grant Action**, and **Deny Action**. When the authentication action is configured as **Grant Action** or **Deny Action**, the client will be granted or denied authentication, regardless of black-list or white-list mode. Only when the action is configured as **Global Action** will the MAC authentication mode be effective. It will be denied in the black-list but granted in the white-list.

Example:

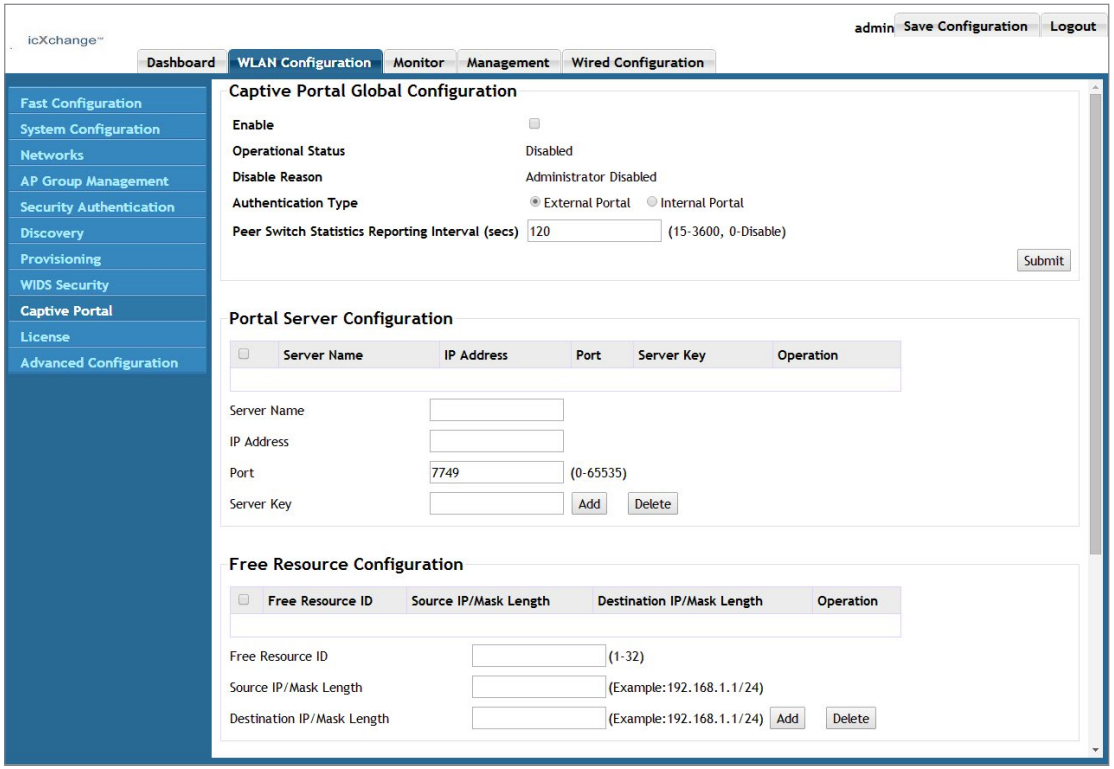
1. Type the client MAC as **00-00-00-00-00-01**, and type the Description as **abcd**. Select the Authentication Action as **Grant Access**, and then click **Add**.
2. Select the added black or white list, and then click **Delete**. Select the **MAC** check box, and then click **Delete**.
3. Click **Modify** to update the client Description and Authentication Action. Click **Submit**.

Note: The MAC address cannot be modified.



Chapter 12: Captive portal

Click **WLAN Configuration->Captive Portal** to open the **Captive Portal Configuration** page. The parameters of portal access authentication can be configured.



12.1 Global configuration

Select the **Enable** check box to enable the captive portal function globally. Clear the check box to disable this function. This function includes the captive portal function on the Link1000ACS and AP.

12.2 Captive portal authentication type

Captive Portal Authentication Type includes an external and internal portal. Select **Internal Portal** or **External Portal** to choose the captive portal authentication type.

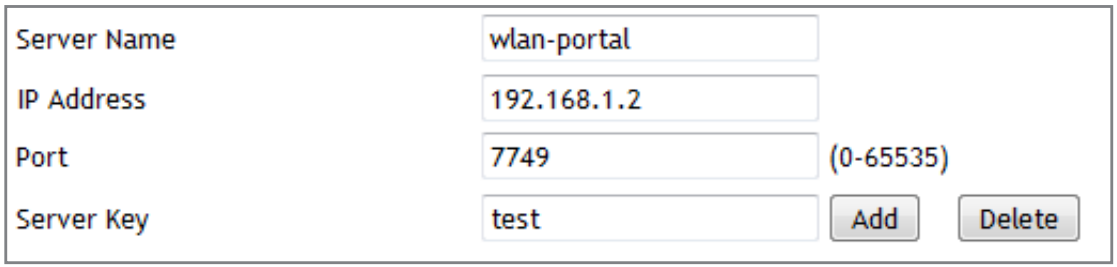
12.3 Portal server configuration

Portal Server Configuration will add or delete the portal Server Name, IP Address, Port, and Server Key.

- Server Name – the name of the appointed portal server
- IP Address – the portal server's IP address
- Port – the port that is monitored when the portal server receives the packet; must be configured according to the actual monitored port (monitored port of DCSM is 50100 and is 2000 for CITY-HOT)
- Server Key – configures the portal server authentication key

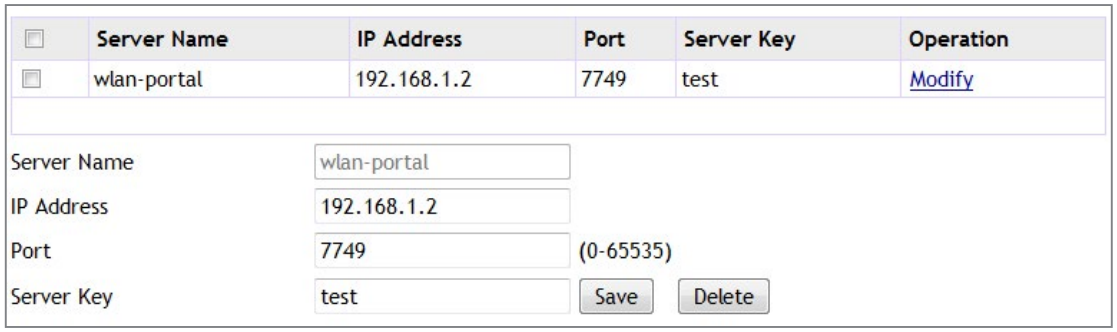
Example:

1. Type the portal Server Name as **wlan_portal**, the IP Address as **192.168.1.2**, the Port as **7749**, and the Server Key as **test**. Click **Add** to complete the configuration.
2. Select the portal server to be deleted, and then click **Delete**.



3. Click **Modify** to the right of the portal server of wlan_portal to modify the IP Address, Port, and Server Key.

Note: The Server Name cannot be modified.



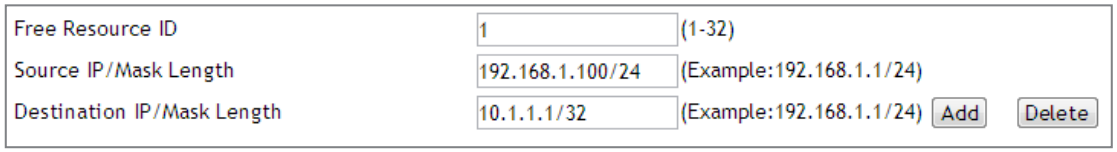
12.4 Free resource configuration

The **Free Resource Configuration** is a walled garden function used to access the free resource in the **Captive Portal** module. Configuring this rule allows a specific client to access the specific network resource without portal authentication.

- Free Resource ID – free resource rule number, ranges from 1 to 32
- Source IP/Mask Length – source IP address field in the rule and the length of its mask
- Destination IP/Mask Length – destination IP address field in the rule and the length of its mask

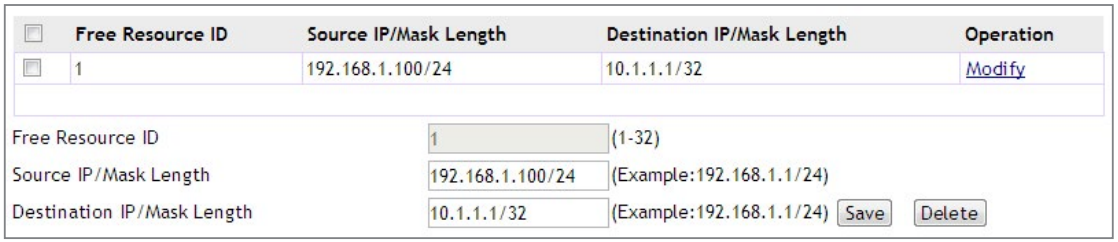
Example:

1. Type the Free Resource ID as **1**, the Source IP/Mask Length as **192.168.1.100/24**, and the Destination IP/Mask Length as **10.1.1.1/32**. Click **Add** to complete the configuration.
2. Select the free resource rule to be deleted, and click **Delete**.



3. Click **Modify** to the right of the Free Resource ID to modify the source IP/Mask Length and the Destination IP/Mask Length.

Note: The Free Resource ID cannot be modified.



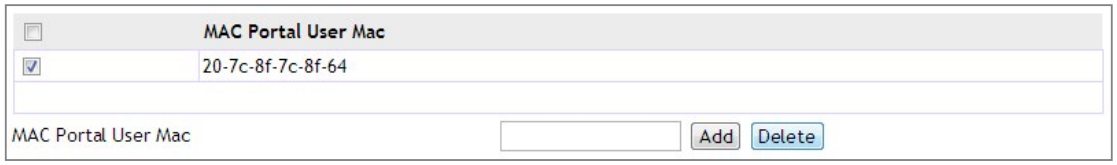
12.5 MAC portal configuration

The **MAC Portal** function is used for special users in the network. The administrator can configure some users to let them connect to the network without portal authentiction. Only the MAC authentication is needed to access all resources.

Click **Captive Portal->MAC Portal Configuration** to add or delete the MAC address of the MAC portal user.

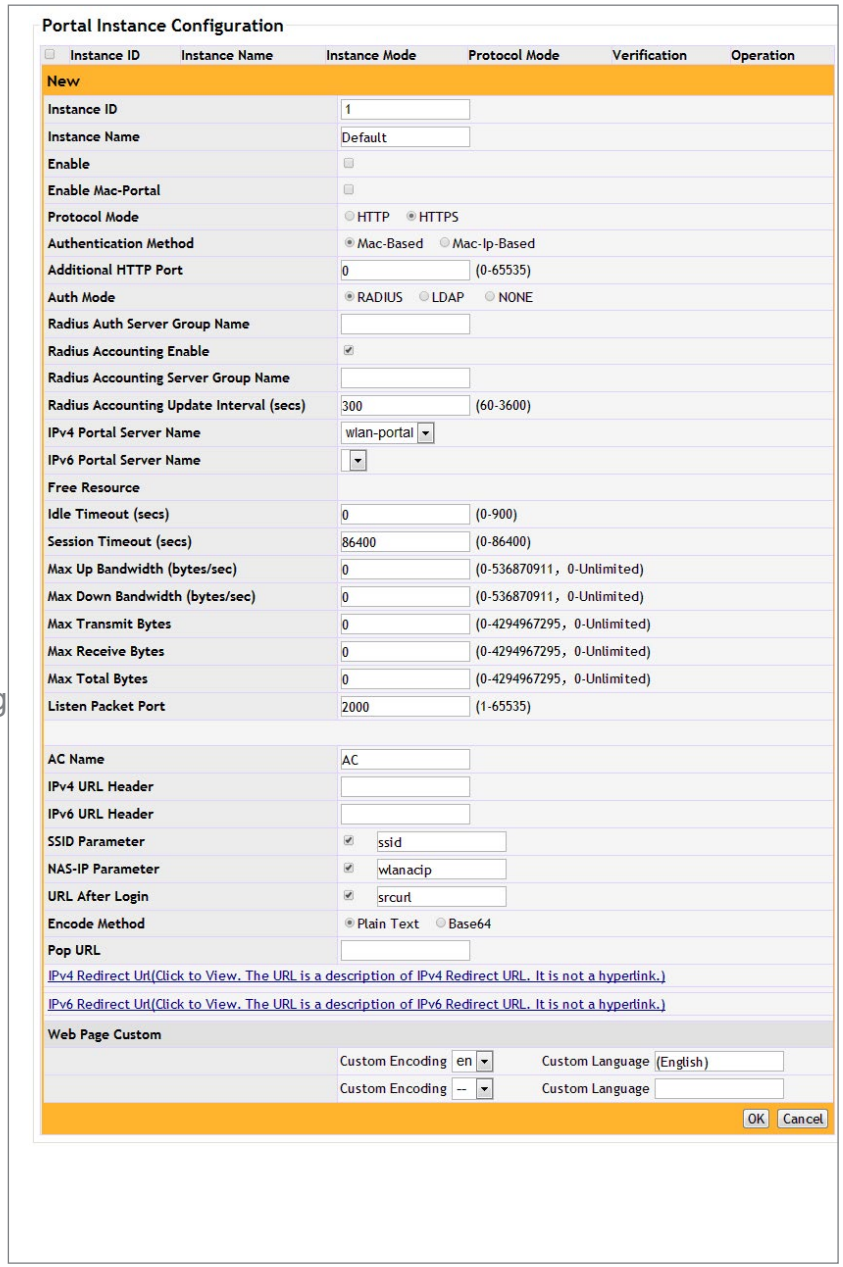
Example:

1. Type the MAC Portal User MAC as **20-7c-8f-7c-8f-64**, and then click **Add**.
2. Select the MAC portal user MAC to be deleted, and then click **Delete**.



12.6 Portal instance configuration

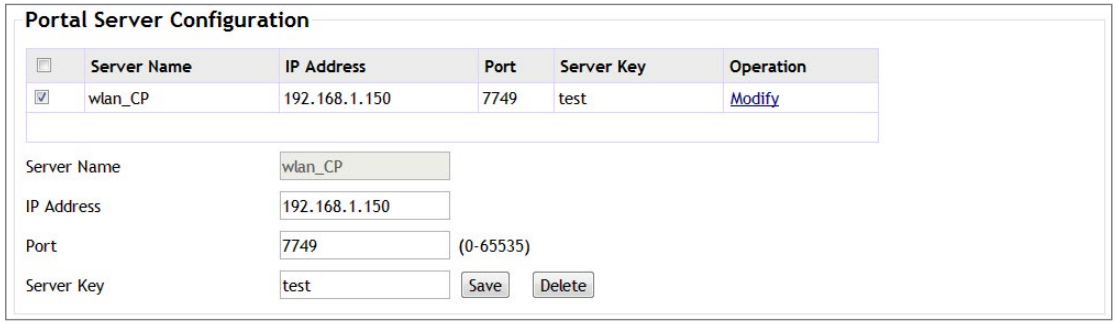
- Instance ID – configures the Captive Portal ID; ranges from 1 to 10. The system supports 10 CP configurations at most.
- Instance Name – appoint a CP name.
- Protocol Mode – the protocol mode that the CP supports. It includes HTTP and HTTPS.
- Authentication Method – includes authentication based on MAC and authentication based on MAC and IP.
- Additional HTTP port – configures the additional HTTP port. It does not include 80 and 443; 0 is the default value, which means that there is no additional HTTP port and it adopts the default 80 port.
- Auth Mode – configures the authentication mode that the CP supports and includes RADIUS, LDAP, and NONE.
- Radius Auth Server Group Name – appoints the Radius authentication server to be used.
- Radius Accounting Server Group Name – appoints the Radius accounting server to be used.
- Radius Accounting Update Interval (secs) – configures the updating interval of the Radius accounting.
- IPv4 Portal Server – appoints the IPv4 portal server to be used.
- IPv6 Portal Server – appoints the IPv6 portal server to be used.
- Free Resource – binds the free resource rule for the CP.
- Idle Timeout (secs) – the idle timeout of CP; 0 is the default value, which means that there is no time limit.
- Session Timeout (secs) – the session timeout of CP; 86400 (24 hours) is the default value, and 0 means that there is no session limitation.



- Max Up Bandwidth (bytes/sec) – configures the user's max up bandwidth. The default value is 0, which means that there is no bandwidth limit.
- Max Down Bandwidth (bytes/sec) – configures the user's max down bandwidth. The default value is 0, which means that there is no bandwidth limit.
- Max Transmit Bytes – configures the max bytes that the user allows to be sent. The default value is 0, which means that there is no byte limit.
- Max Receive Bytes – configures the max bytes that the user allows to be received. The default value is 0, which means that there is no byte limit.
- Max Total Bytes – configures the max bytes that the user allows to be sent and received. The default value is 0, which means that there is no byte limit.
- Listen Packet Port – configures the port that is listened to when portal server receives the packet.

Example:

1. Click **Add**, and type the Instance ID and Instance Name. Enable the captive portal configuration, and then select the Auth Mode and other parameters as needed. Click **OK** to complete the captive portal configuration.
2. Click **Modify** to modify the wlan_CP configuration.



3. Select the added CP, and click **Delete** to delete it.

Chapter 13: Configuration push

Click **WLAN Configuration->WLAN Advanced Configuration->Configuration Push** to open the **Configuration Push** page, which includes two modules: **Configuration Push** and **Configuration Push Option**. The user can select the other Link1000ACSs in the cluster, configure each of the options to be pushed, and configure to push.

13.1 Configuration push

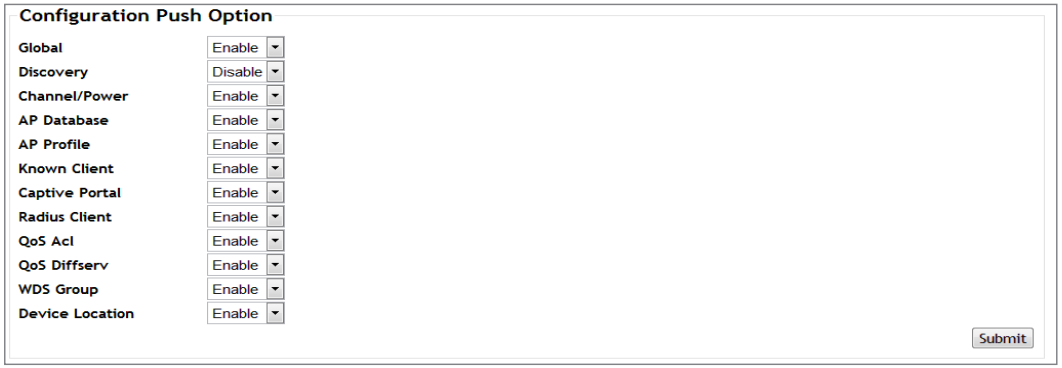
Configuration Push displays the IP address of the Link1000ACSs in the cluster. One Link1000ACS can be selected to run the **Configuration Push**; clicking **All Push** can update all ACs in the current cluster.

IP Address is for the peer switch; the configuration can be pushed to these two switches. If there is no other switch in the cluster, the **IP Address** bar is empty. In this scenario, **Configuration Push** cannot be run.

13.2 Configuration push option

Configuration Push Option is used to configure the configuration transferred by **Configuration Push**. Every option is hidden as default. Click **Configuration Push Option** to open it, and click **Hide Push Option** to hide the status.

After opening the **Configuration Push Option**, select **Enable** or **Disable** for each option.

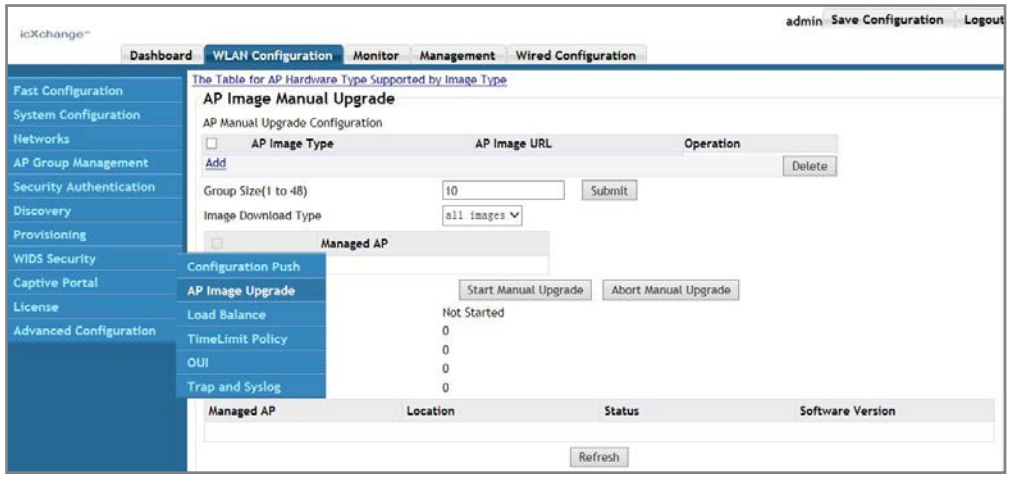


Click **Submit**, and the configuration will be saved.

Chapter 14: AP image upgrade

14.1 AP manual upgrade configuration

In **AP Manual Upgrade Configuration**, the controller loads an AP firmware version file directly to single or multiple APs to perform firmware updates.

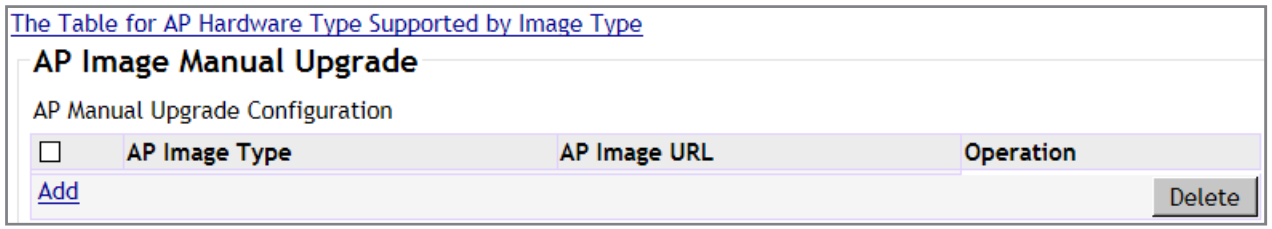


1. Click **The Table for AP Hardware Type Supported by Image Type** link to determine the hardware type. Click **Hide The Table for AP Hardware Type Supported by Image Type** to hide this information on the screen.

Hide The Table for AP Hardware Type Supported by Image Type

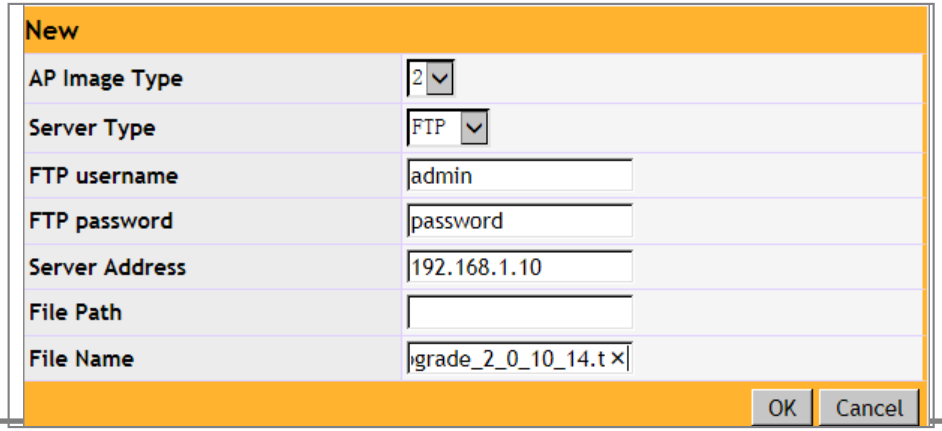
AP Image Type	Device-type List
1	Supported AP Hardware Type: N/A
2	Supported AP Hardware Type: 5 7 21 22 23
3	Supported AP Hardware Type: N/A
4	Supported AP Hardware Type: N/A
5	Supported AP Hardware Type: 26

2. Click **Add** to start the AP image URL Configuration.

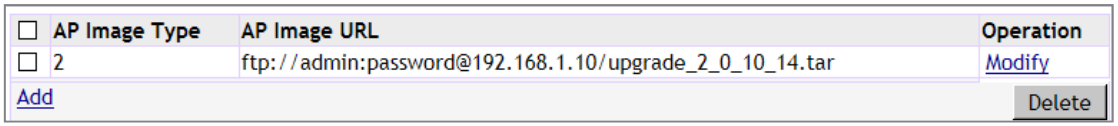


The following page will generate:

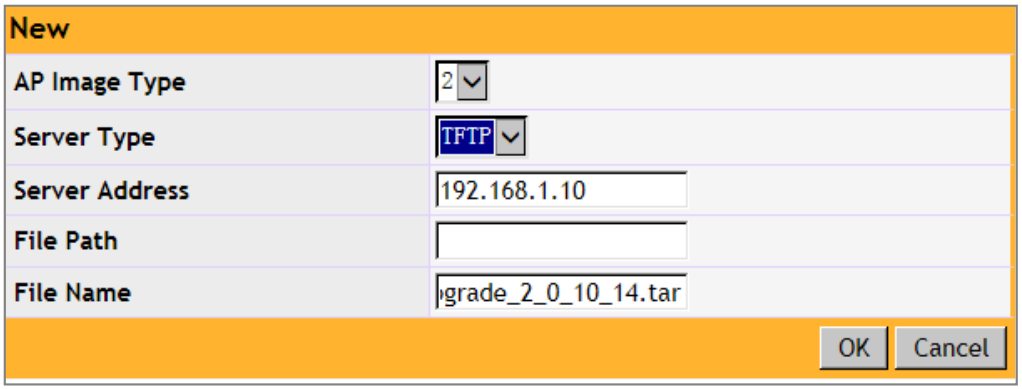
Select an image type from the **AP Image Type** drop-down list. From the **Server Type** drop-down list, select **FTP** or **TFTP**. The following figure shows the FTP configuration:



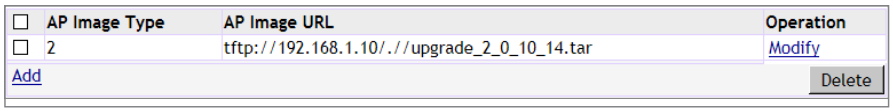
The FTP username and password should be consistent. If the file is in the server root directory, it cannot be typed. If it is not in the root directory, the File Name should be entered. Click **OK** to complete this configuration.



The following figure shows the TFTP configuration.

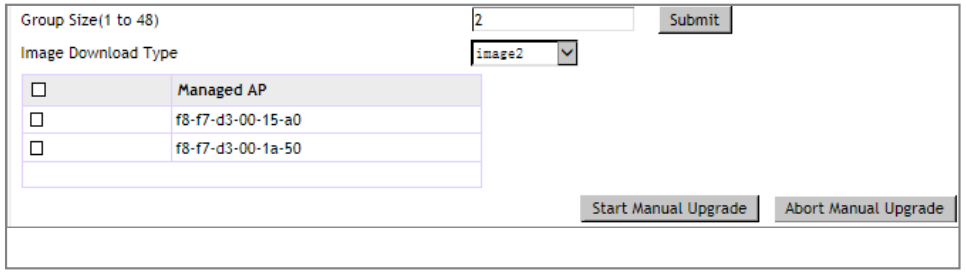


Configure the Server Address and File Name. If the file is in the server root directory, it cannot be typed. If it is not in the root directory, the File Name should be entered. Click **OK** to complete this configuration.



To delete or modify a configured AP image URL, select it, and then click **Delete** or **Modify**.

3. After configuring the AP Image URL, configure the Group Size and Image Download Type.

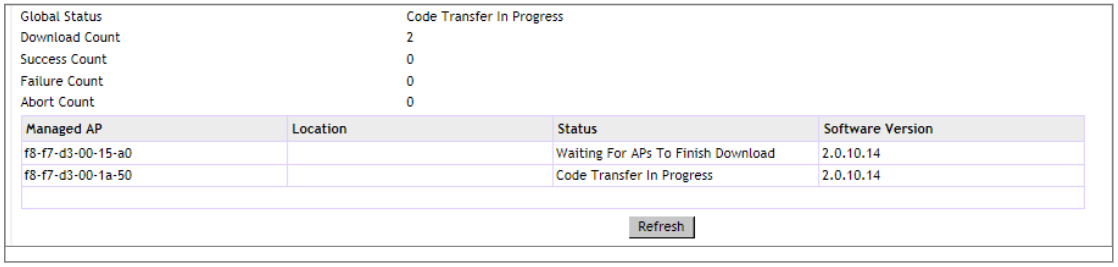


- Group Size: the number of simultaneous FTP or TFTP threads to update in the batch.
- Image Download Type: click the proper Image Download Type to upgrade the AP with the specific image type. The **Image Download Type** drop-down list includes **none, 1–5**, and **all images**. Image type will default to **all images** by clicking the **Submit** button.
  - **none** will upgrade only one AP
  - **all images** will upgrade all types of images
  - **other options** will upgrade a specific type of image

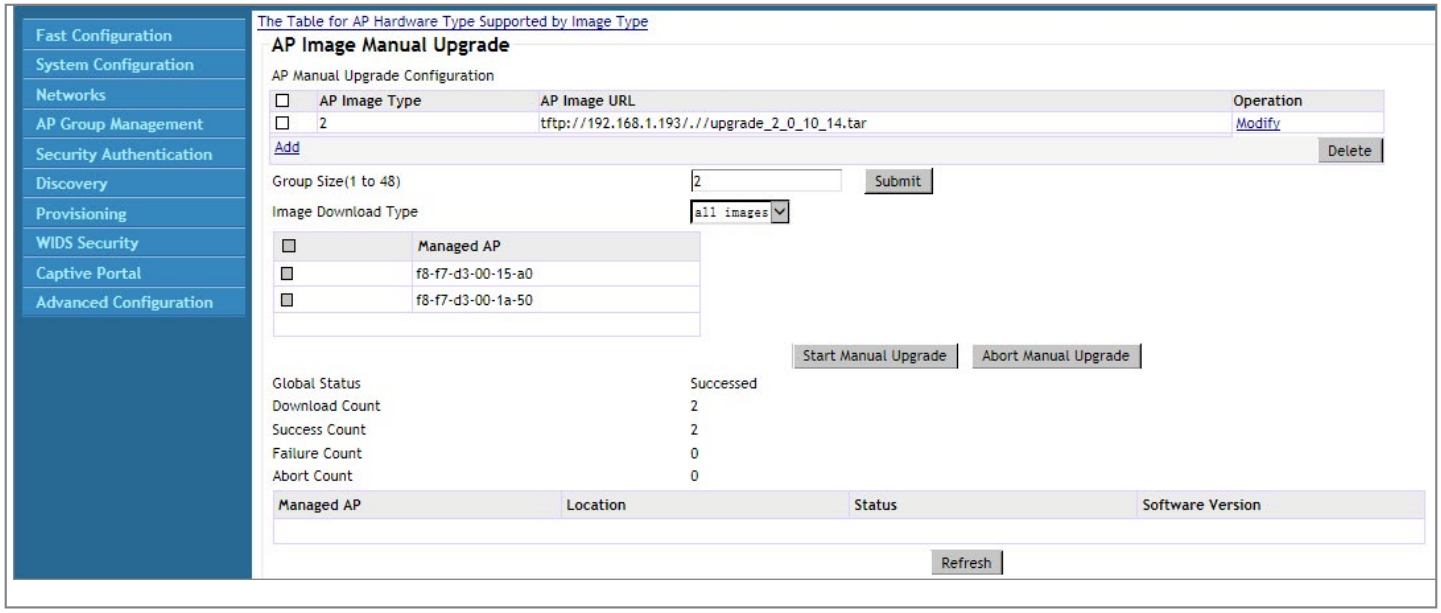
Click **Submit** to set the batch job.

4. Click **Start Manual Upgrade** to begin the AP upgrade. Click **Abort Manual Upgrade** to cancel it.

5. After beginning the upgrade, the Status is shown, as in the following figure:



When the upgrade is complete, the following window will appear:



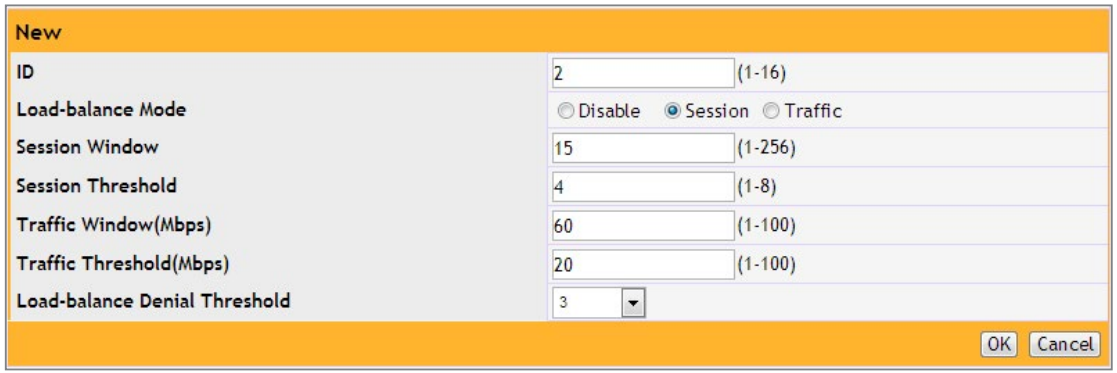
Chapter 15: Load balance

Click **WLAN Configuration->Advanced Configuration->Load Balance** to open up the **Load Balance Configuration** page to configure parameters.

15.1 Create template

The **Load Balance Template 1** is disabled by default, and it cannot be deleted.

Click **New** to configure the new Load Balance Template. The new ID cannot be the same as the existing ID:



The load balance includes **Session** and **Traffic**. These two modes correspond respectively to the two parameters threads, as shown in the previous figure.

Session mode displays the allowed client association, based on the number of associated users. **Traffic** mode displays the allowed client association, based on the maximum bandwidth utilization of the configured radio interface.

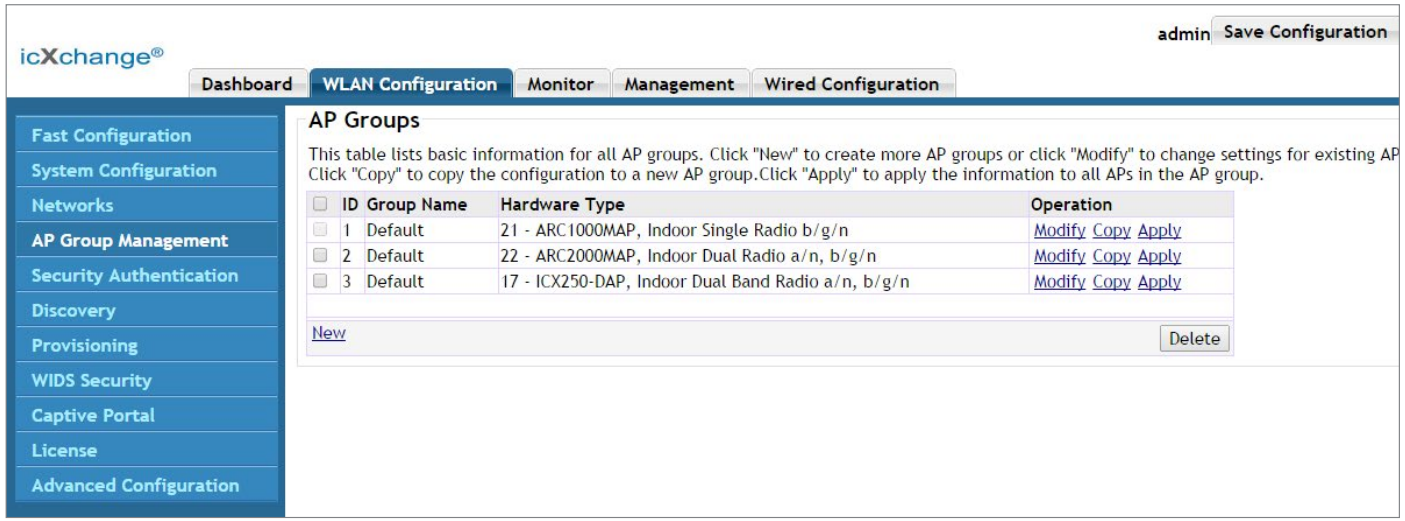
Load-balance Denial Threshold is the amount of times that the AP can refuse the client before receiving its association request.

The Link1000ACS will decide client association based on the number of clients in the current WLAN system. At the same time, it will monitor the radio interface load on the local AP. When the load exceeds the maximum value, it will send a trap to network management. It can also force clients to be released when it discovers these clients exceed the maximum value.

15.2 AP profile associated load balance template

After creating the Load Balance Template, the template must be added to the AP profile in **AP Group Management**, and the configuration must be pushed to AP group by clicking the **Apply** link. After this procedure is complete, the template will be effective.

Click **WLAN Configuration->AP Group Management** to find the group ID (AP profile) to be bound to the load balance, and then click **Modify**.


admin
Save Configuration
icXchange
Dashboard
WLAN Configuration
Monitor
Management
Wired Configuration
Fast Configuration
System Configuration
Networks
AP Group Management
Security Authentication
Discovery
Provisioning
WIDS Security
Captive Portal
License
Advanced Configuration
AP Groups
This table lists basic information for all AP groups. Click "New" to create more AP groups or click "Modify" to change settings for existing AP
Click "Copy" to copy the configuration to a new AP group.Click "Apply" to apply the information to all APs in the AP group.
ID Group Name Hardware Type Operation
1 Default 21 - ARC1000MAP, Indoor Single Radio b/g/n Modify Copy Apply
2 Default 22 - ARC2000MAP, Indoor Dual Radio a/n, b/g/n Modify Copy Apply
3 Default 17 - ICX250-DAP, Indoor Dual Band Radio a/n, b/g/n Modify Copy Apply
New
Delete

Scroll down to **Load Balance Template** and select the template ID created previously from the drop-down list. Click **Save** to save the modification.

After modifying, click **Apply** to the right of that group ID to issue the parameters to one or more APs in this group.

15.3 Delete load balance template

Select one or more templates from the list in the **Load Balance** page, and then click **Delete**. The template that is bound by the AP group cannot be deleted. Release the association with the AP on the **AP Group Management** page, and then click **Delete**.

Note: Template 1 cannot be deleted.

Chapter 16: Data transfer

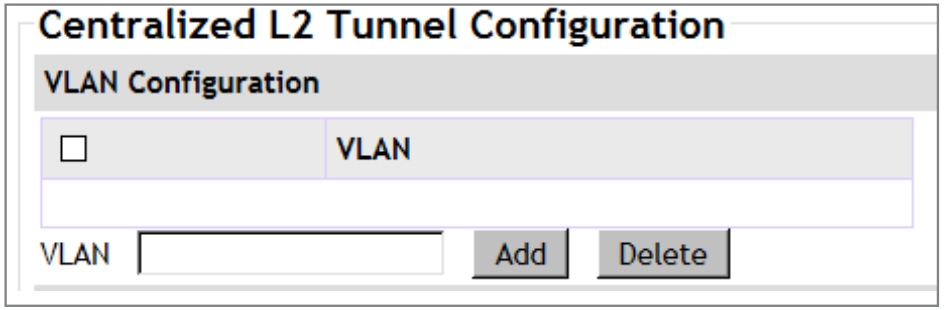
Click **WLAN Configuration->Advanced Configuration->Data Transfer** to configure the Centralized L2 Tunnel Configuration.

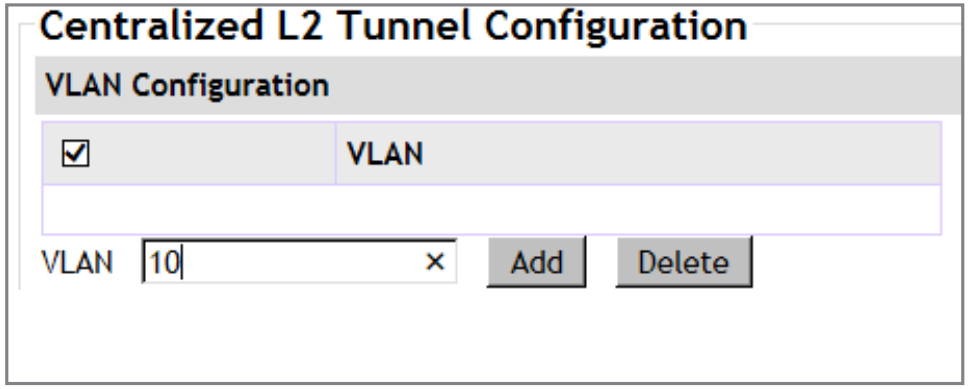
16.1 Centralized L2 tunnel configuration

16.1.1 VLAN config

Add the data VLAN into the centralized tunnel through VLAN Config to achieve the centralized transfer.

Example: Type **10** into the VLAN text box, and then click **Add**.





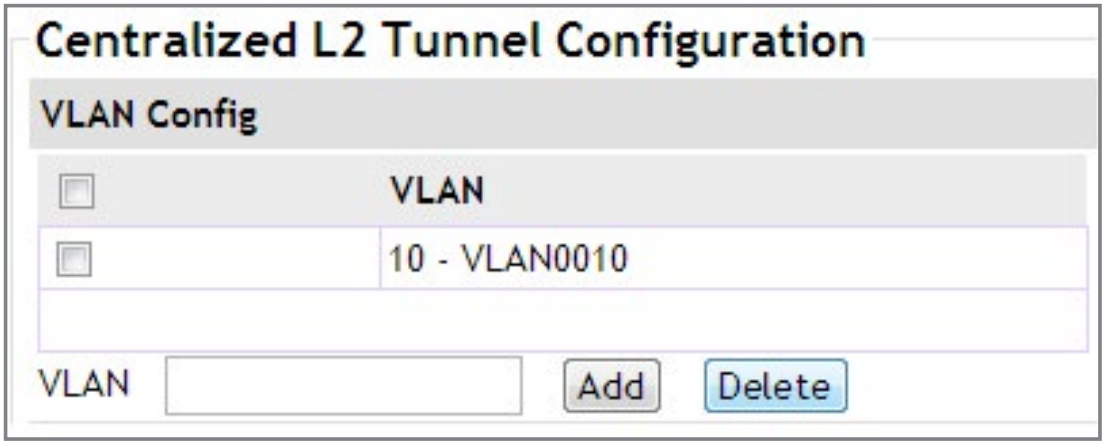
Select **10 - VLAN0010**, and then click **Delete** to delete it.

16.1.2 Station isolation VLAN

The users under the **Station Isolation VLAN** will be isolated from each other. The station isolation VLAN must first exist in the centralized VLAN, and then it can be created and added. From the **Station Isolation VLAN** drop-down list, select **Add**, **Remove**, or **Delete All**.

- **Add**: the VLAN must have been in the centralized tunnel.
- **Remove**: delete one configured station isolation VLAN.
- **Delete all**: delete all isolation VLANs.

Example: Select **10 - VLAN0010**, and then click **Add**. Click **Submit** to confirm changes.



Chapter 17: Time limit policy

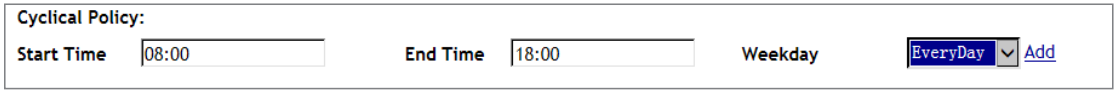
The **Time Limit Policy** configures the user on-line time, including **Network Time Limit Configuration** and **Radio Time Limit Configuration**.

The network time limit configuration is based on the network, and it limits clients' access to the network by disabling VAP. The radio time limit configuration is under the radio, and it limits clients' access to the network by disabling the radio. These two policies include the **Cyclical Policy** and **UTC Policy**. The cyclical policy is used to configure the time of one day or week; for example, stop the network access from hh:mm to hh:mm. The UTC policy is used to configure the detailed date; for example, allow or stop the network access from hh:mm on YYYY-MM-DD to hh:mm on YYYY-MM-DD.

17.1 Network time limit configuration

Select the **Network ID** from the drop-down list to configure the time limit policy under the network to be accessed, and configure the Start Time and End Time of the cyclical policy. In the Weekday column, the user can choose **EveryDay** or a weekday. After configuration, the network cannot be accessed on the specified day(s) during the configured times. In the UTC policy, the Start Time and End Time should be configured as the detailed time. The Network Status includes **Up** and **Down**, which enables or disables the VAP that the network corresponds to in this time.

Example: Configure network 1 to prevent network access from 8:00–18:00 every day, as shown in the following figure:



Click **Add** to complete it.

	Start Time	End Time	Weekday	Network Status
☐	08:00	18:00	EveryDay	Down

Example: Configure network 2 to access the network from 9:00 on May 13, 2013–18:00 on May 18, 2013 as shown in the following figure:

Click **Add** to complete the configuration.

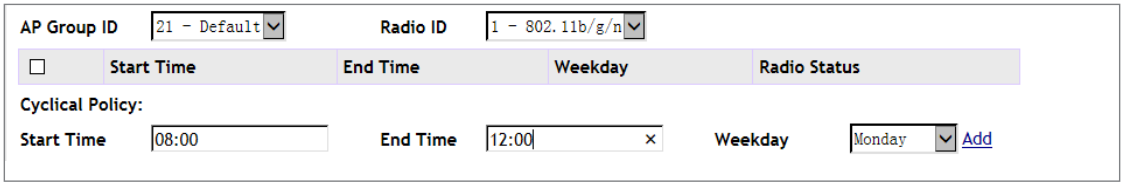
☐	Start Time	End Time	Weekday	Network Status
☐	2013-05-13 09:00	2013-05-18 18:00		Up

Select the configured policy, and then click **Delete** to delete the policy.

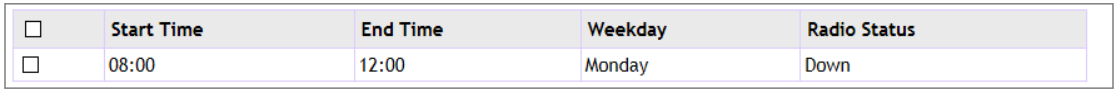
17.2 Radio time limit configuration

Select the **AP Group ID** from the drop-down list to configure the policy under this AP group. Select **Radio ID** from the drop-down list to choose the radio to be configured. The cyclical policy configuration disables this radio and limits the network access in this time. When configuring the UTC policy, the user can select **Up** or **Down** for the radio status, allowing the radio to be enabled or disabled.

Example: Configure radio 21 under profile 1 to disable the VAPS in that group on the cyclical policy from 8:00 to 12:00 every Monday.

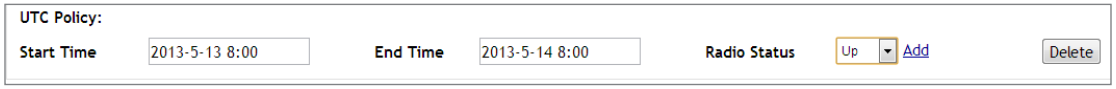


Click **Add** to complete the configuration.

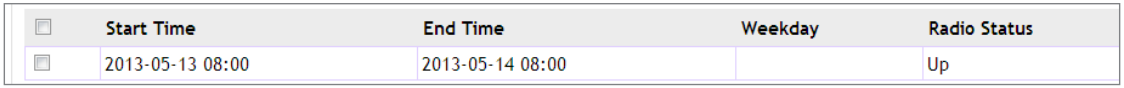


☐	Start Time	End Time	Weekday	Radio Status
☐	08:00	12:00	Monday	Down

Example: Configure the Radio Status as **Up** from 8:00 on May 13, 2013 to 8:00 on May 14, 2013.



Click **Add** to complete the configuration.

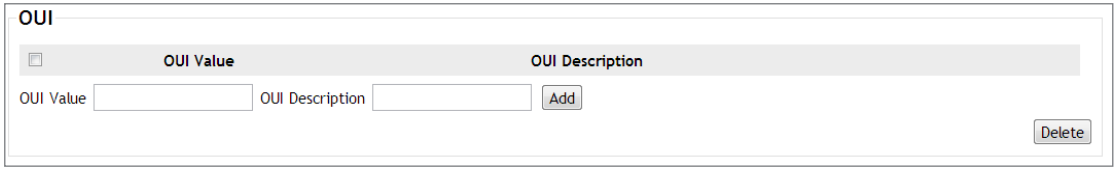


To delete the policy, select the configured policy, and then click **Delete**.

Chapter 18: Organization unique identifier (OUI)

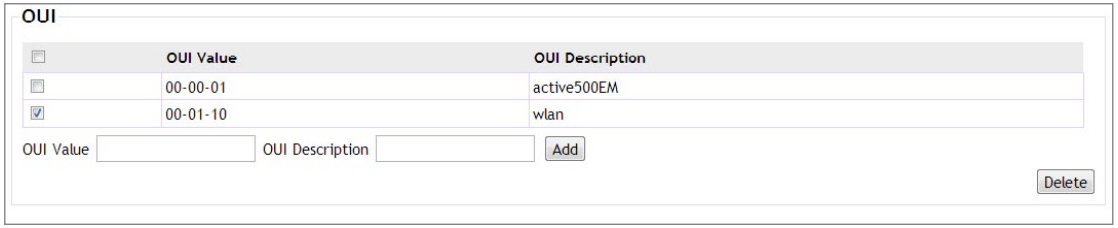
18.1 Add OUI

Click **WLAN Configuration->WLAN Advanced Configuration->OUI** to type the OUI Value (its format is xx-xx-xx). Type the OUI Description, and then click **Add**.



18.2 Delete OUI

Click **WLAN Configuration->WLAN Advanced Configuration->OUI**. Select the OUI to be deleted, and click **Delete**.



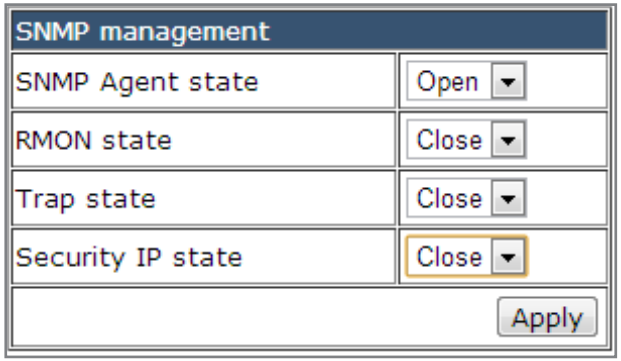
Chapter 19: Trap and syslog

Click **WLAN Configuration->Advanced Configuration->Trap and Syslog** to open the **Trap and Syslog Configuration** page for the SNMP trap and syslog configuration.

19.1 SNMP traps

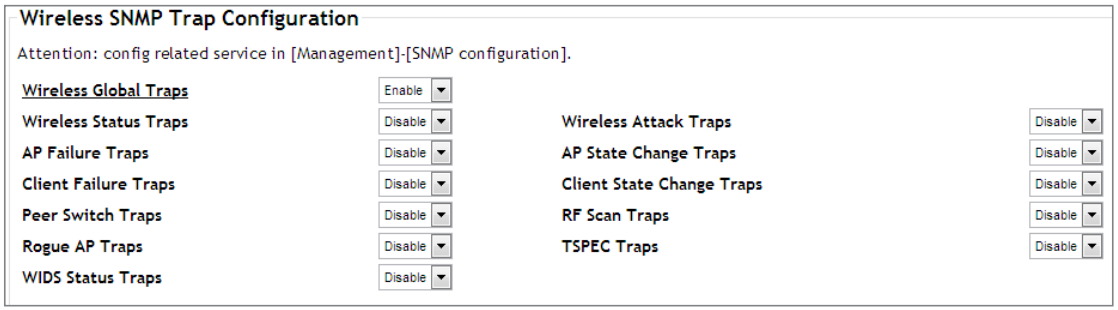
Prior to enabling SNMP trap, configure the items in the **SNMP management** dialog box .

On the **Management->SNMP Configuration->SNMP Management** page, select **Open** for the SNMP Agent state, and then click **Apply** to enable the SNMP management on/off.



19.1.1 Wireless global traps

On the **SNMP Trap Configuration** page, select **Enable** for Wireless Global Traps. After enabling the wireless global traps, enable or disable each trap option.



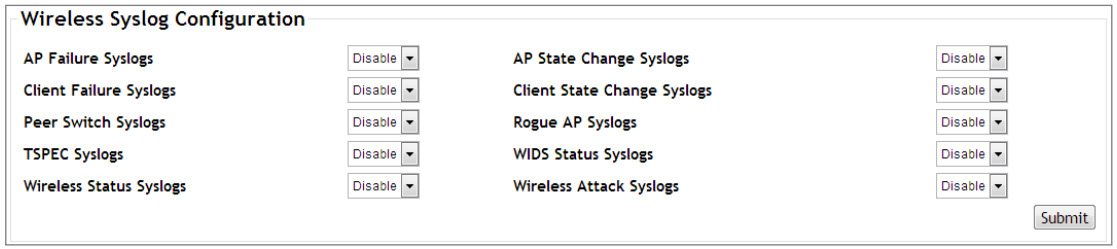
Click **Submit** to save the configuration. Each wireless trap will be effective only after the Wireless Global Traps On/Off is enabled. Users can view the configuration on the **Network Management** page.

19.2 Syslog configuration

View the syslog information on the syslog server through the Syslog Configuration.

19.2.1 Wireless syslog configuration

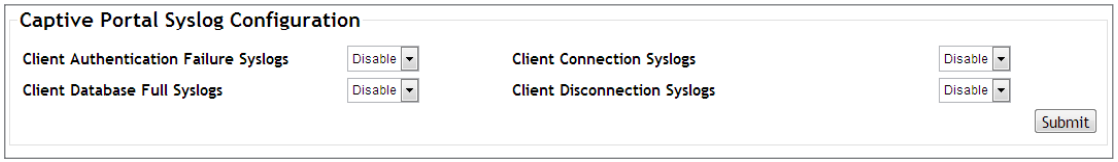
On the **Wireless Syslog Configuration** page, select the available options from the drop-down menu to enable/disable the wireless syslog.



After configuring, click **Submit** to save the configuration. Users can view the configured wireless syslog on the syslog server.

19.2.2 Captive portal syslog configuration

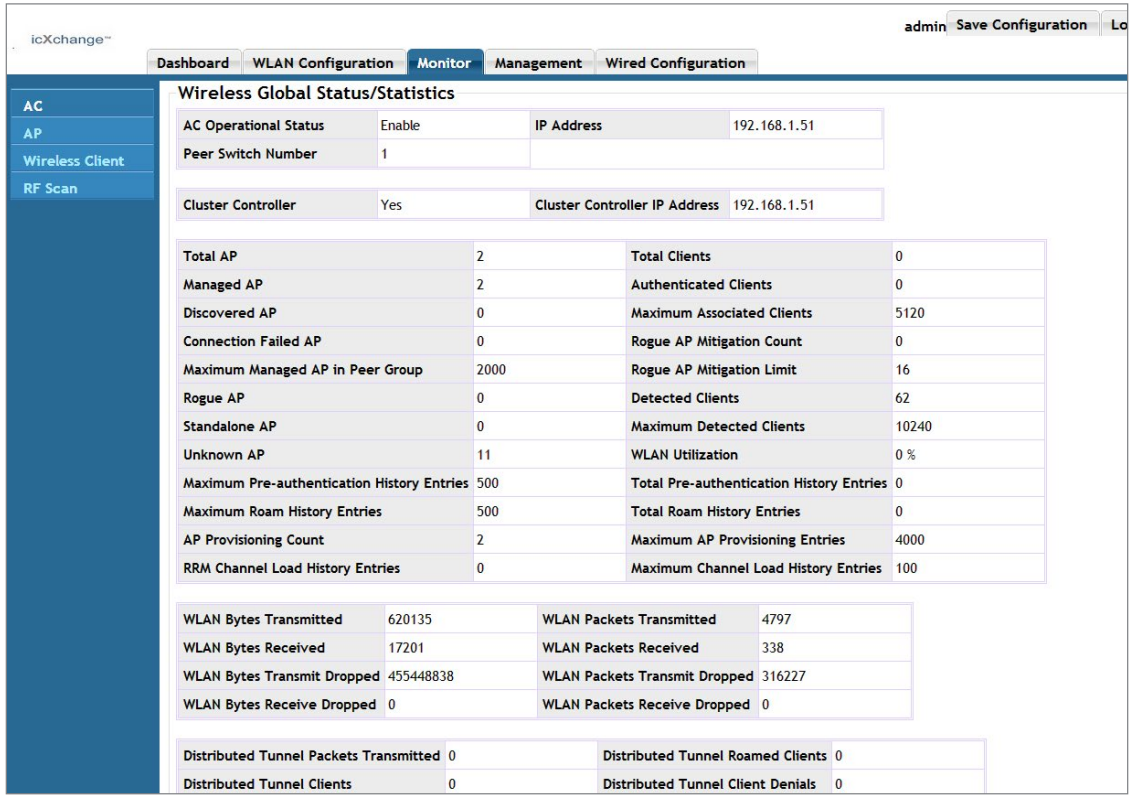
On the **Captive Portal Syslog Configuration** page, select to enable or disable each option of the captive portal syslog.



After configuring, click **Submit** to save the configuration. Users can view the enabled captive portal syslog on the syslog server.

Chapter 20: Monitor

Click **Monitor** to view and monitor the **AC, AP, Wireless Client**, and **RF Scan**.

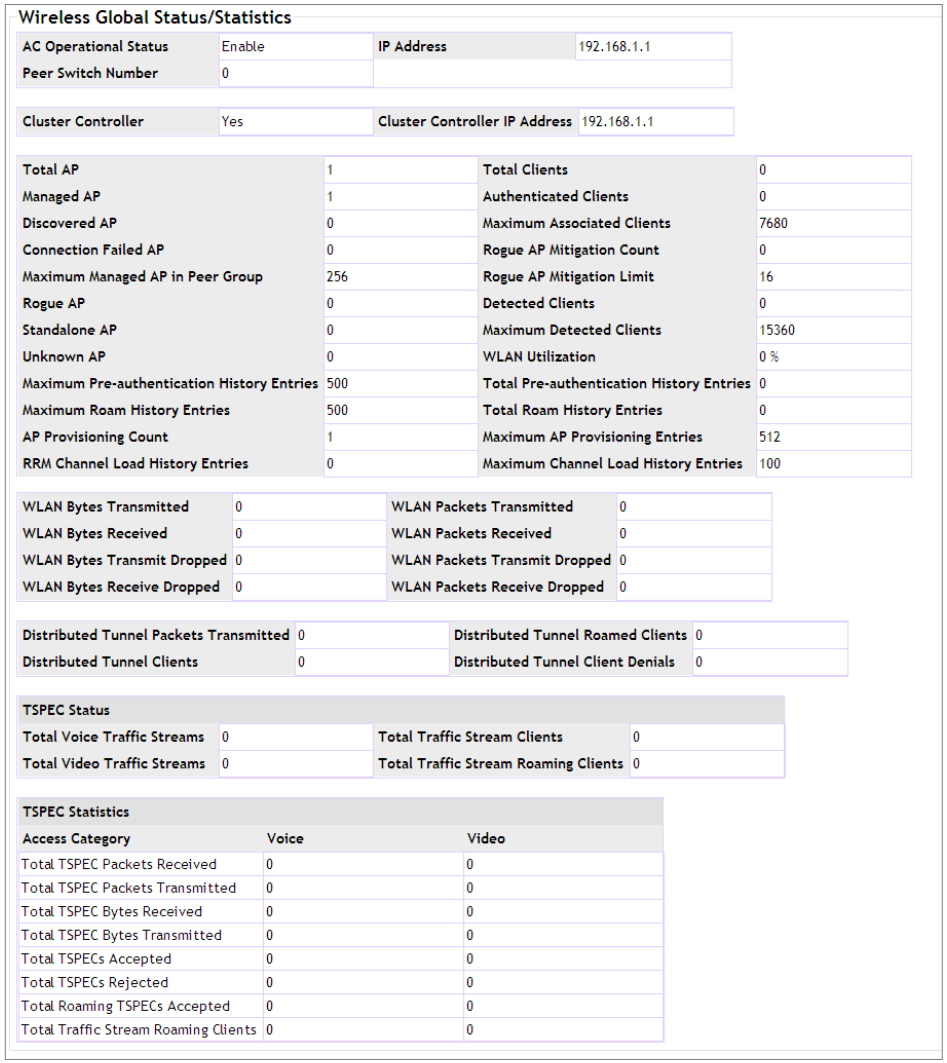


20.1 AC

Click **Monitor->Link1000ACS** to open the **Link1000ACS Monitor** page to monitor the cluster and status/statistics.

20.1.1 Cluster

Click **Monitor->Link1000ACS** to open the **Link1000ACS Monitor** page to view the cluster information including the Link1000ACS **Operational Status**, **Cluster Controller**, **Basic Information**, **Global Statistics**, **Distributed Tunnel Statistics**, **TSPEC Status**, and **TSPEC Statistics**.



Wireless Global Status/Statistics

AC Operational Status	Enable	IP Address	192.168.1.1
Peer Switch Number	0		

Cluster Controller	Yes	Cluster Controller IP Address	192.168.1.1

Total AP	1	Total Clients	0
Managed AP	1	Authenticated Clients	0
Discovered AP	0	Maximum Associated Clients	7680
Connection Failed AP	0	Rogue AP Mitigation Count	0
Maximum Managed AP in Peer Group	256	Rogue AP Mitigation Limit	16
Rogue AP	0	Detected Clients	0
Standalone AP	0	Maximum Detected Clients	15360
Unknown AP	0	WLAN Utilization	0 %
Maximum Pre-authentication History Entries	500	Total Pre-authentication History Entries	0
Maximum Roam History Entries	500	Total Roam History Entries	0
AP Provisioning Count	1	Maximum AP Provisioning Entries	512
RRM Channel Load History Entries	0	Maximum Channel Load History Entries	100

WLAN Bytes Transmitted	0	WLAN Packets Transmitted	0
WLAN Bytes Received	0	WLAN Packets Received	0
WLAN Bytes Transmit Dropped	0	WLAN Packets Transmit Dropped	0
WLAN Bytes Receive Dropped	0	WLAN Packets Receive Dropped	0

Distributed Tunnel Packets Transmitted	0	Distributed Tunnel Roamed Clients	0
Distributed Tunnel Clients	0	Distributed Tunnel Client Denials	0

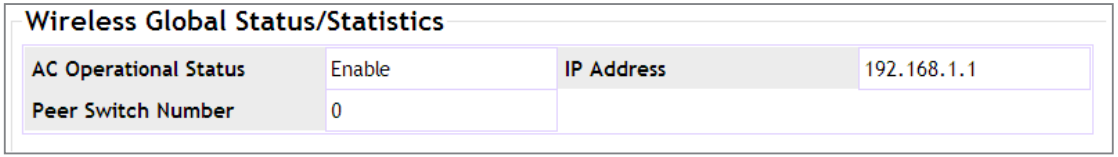
TSPEC Status			
Total Voice Traffic Streams	0	Total Traffic Stream Clients	0
Total Video Traffic Streams	0	Total Traffic Stream Roaming Clients	0

TSPEC Statistics

Access Category	Voice	Video
Total TSPEC Packets Received	0	0
Total TSPEC Packets Transmitted	0	0
Total TSPEC Bytes Received	0	0
Total TSPEC Bytes Transmitted	0	0
Total TSPECs Accepted	0	0
Total TSPECs Rejected	0	0
Total Roaming TSPECs Accepted	0	0
Total Traffic Stream Roaming Clients	0	0

20.1.1.1 The Link1000ACS operational status

Wireless Global Status/Statistics in the cluster includes the Link1000ACS **Operational Status**, **IP Address**, and **Peer Switch Number**. The IP address is the wireless IP address, as shown in the following figure:



20.1.1.2 Cluster controller

- Cluster Controller – displays **Yes** or **No**. **Yes** indicates that the local Link1000ACS is the cluster controller; **No** indicates that it is not the cluster controller.
- Cluster Controller IP Address – the wireless address of the cluster controller.

20.1.1.3 Local Link1000ACS information

The Link1000ACS Information includes **Total AP**, **Managed AP**, **Discovered AP**, **Connection Failed AP**, **Maximum Managed AP in Peer Group**, etc. It also includes **Total Clients**, **Authenticated Clients**, **Detected Clients**, **WLAN Utilization**, etc. The figure is as follows:

Total AP	1	Total Clients	0
Managed AP	1	Authenticated Clients	0
Discovered AP	0	Maximum Associated Clients	7680
Connection Failed AP	0	Rogue AP Mitigation Count	0
Maximum Managed AP in Peer Group	256	Rogue AP Mitigation Limit	16
Rogue AP	0	Detected Clients	19
Standalone AP	0	Maximum Detected Clients	15360
Unknown AP	5	WLAN Utilization	0 %
Maximum Pre-authentication History Entries	500	Total Pre-authentication History Entries	0
Maximum Roam History Entries	500	Total Roam History Entries	0
AP Provisioning Count	1	Maximum AP Provisioning Entries	512
RRM Channel Load History Entries	0	Maximum Channel Load History Entries	100

20.1.1.4 Global Statistics

The Global Statistics of the local Link1000ACS is shown as follows:

WLAN Bytes Transmitted	0	WLAN Packets Transmitted	0
WLAN Bytes Received	77672	WLAN Packets Received	200
WLAN Bytes Transmit Dropped	4971156	WLAN Packets Transmit Dropped	3888
WLAN Bytes Receive Dropped	0	WLAN Packets Receive Dropped	0

20.1.1.5 Distributed tunnel statistics

The Distributed Tunnel Statistics of the local Link1000ACS is shown as follows:

Distributed Tunnel Packets Transmitted	0	Distributed Tunnel Roamed Clients	0
Distributed Tunnel Clients	0	Distributed Tunnel Client Denials	0

20.1.1.6 TSPEC status

The TSPEC Status of the Link1000ACS is shown as follows:

TSPEC Status			
Total Voice Traffic Streams	0	Total Traffic Stream Clients	0
Total Video Traffic Streams	0	Total Traffic Stream Roaming Clients	0

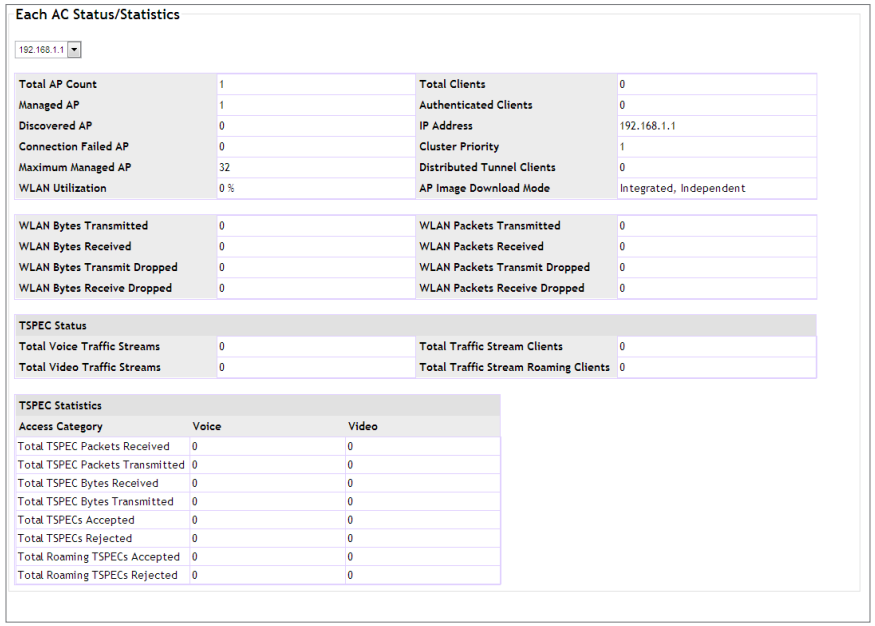
20.1.1.7 TSPEC Statistics

The TSPEC Statistics of the Link1000ACS is shown as follows:

TSPEC Statistics		
Access Category	Voice	Video
Total TSPEC Packets Received	0	0
Total TSPEC Packets Transmitted	0	0
Total TSPEC Bytes Received	0	0
Total TSPEC Bytes Transmitted	0	0
Total TSPECs Accepted	0	0
Total TSPECs Rejected	0	0
Total Roaming TSPECs Accepted	0	0
Total Traffic Stream Roaming Clients	0	0

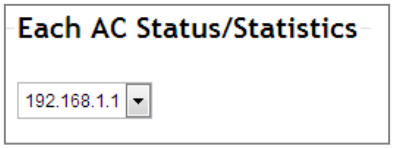
20.1.2 Each AC status/statistics

Click **Monitor->AC** to open the **Link1000ACS Monitor** page. Scroll down to view **Each AC Status/Statistics**. Use the drop-down box to access clustered ACs. Infomation includes basic AC information, AC statistics, TSPEC status and TSPEC statistics. It can monitor the Link1000ACS status.


Each AC Status/Statistics
192.168.1.1
Total AP Count 1
Managed AP 1
Discovered AP 0
Connection Failed AP 0
Maximum Managed AP 32
WLAN Utilization 0 %
Total Clients 0
Authenticated Clients 0
IP Address 192.168.1.1
Cluster Priority 1
Distributed Tunnel Clients 0
AP Image Download Mode Integrated, Independent
WLAN Bytes Transmitted 0
WLAN Bytes Received 0
WLAN Bytes Transmit Dropped 0
WLAN Bytes Receive Dropped 0
WLAN Packets Transmitted 0
WLAN Packets Received 0
WLAN Packets Transmit Dropped 0
WLAN Packets Receive Dropped 0
TSPEC Status
Total Voice Traffic Streams 0
Total Video Traffic Streams 0
Total Traffic Stream Clients 0
Total Traffic Stream Roaming Clients 0
TSPEC Statistics
Access Category Voice Video
Total TSPEC Packets Received 0 0
Total TSPEC Packets Transmitted 0 0
Total TSPEC Bytes Received 0 0
Total TSPEC Bytes Transmitted 0 0
Total TSPECs Accepted 0 0
Total TSPECs Rejected 0 0
Total Roaming TSPECs Accepted 0 0
Total Roaming TSPECs Rejected 0 0

20.1.2.1 AC selection list

In the AC IP Address Selection list, select the IP address from the drop-down box to view the corresponding AC status/statistics, as shown in the following figure:



20.1.2.2 Basic AC information

Basic AC information includes **Total AP Count**, **Managed AP**, **Discovered AP**, **Connection Failed AP**, **Maximum Managed AP**, **Total Clients**, **Cluster Priority**, **AP Image Download Mode**, **WLAN Utilization**, etc. , as shown in the following figure:

Total AP Count	1	Total Clients	0
Managed AP	1	Authenticated Clients	0
Discovered AP	0	IP Address	192.168.1.1
Connection Failed AP	0	Cluster Priority	0
Maximum Managed AP	32	Distributed Tunnel Clients	0
WLAN Utilization	0 %	AP Image Download Mode	Integrated, Independent

20.1.2.3 AC statistics

AC Statistics are shown as follows:

WLAN Bytes Transmitted	0	WLAN Packets Transmitted	0
WLAN Bytes Received	77672	WLAN Packets Received	200
WLAN Bytes Transmit Dropped	4971156	WLAN Packets Transmit Dropped	3888
WLAN Bytes Receive Dropped	0	WLAN Packets Receive Dropped	0

20.1.2.4 TSPEC Status

The TSPEC Status is shown as follows:

TSPEC Status			
Total Voice Traffic Streams	0	Total Traffic Stream Clients	0
Total Video Traffic Streams	0	Total Traffic Stream Roaming Clients	0

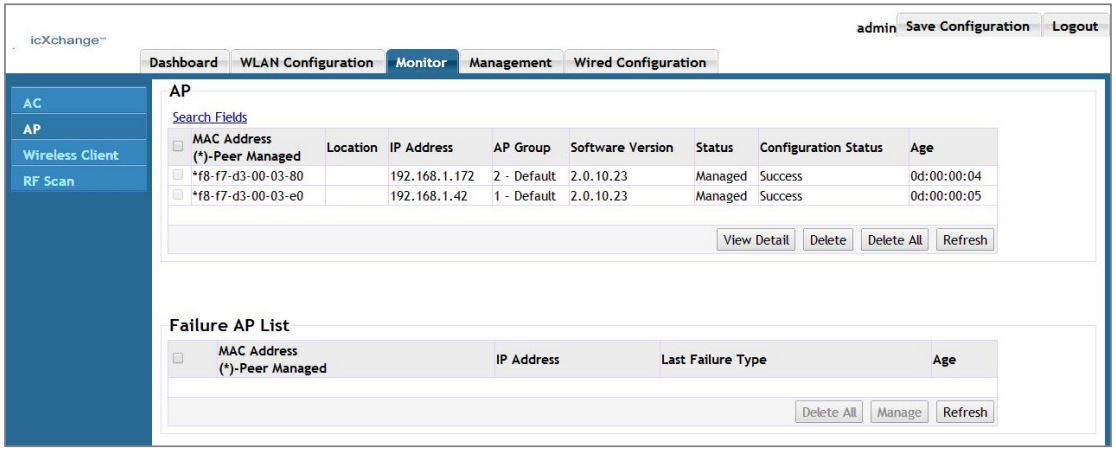
20.1.2.5 TSPEC Statistics

The TSPEC Statistics is shown as follows:

TSPEC Statistics		
Access Category	**Voice**	**Video**
Total TSPEC Packets Received	0	0
Total TSPEC Packets Transmitted	0	0
Total TSPEC Bytes Received	0	0
Total TSPEC Bytes Transmitted	0	0
Total TSPECs Accepted	0	0
Total TSPECs Rejected	0	0
Total Roaming TSPECs Accepted	0	0
Total Traffic Stream Roaming Clients	0	0

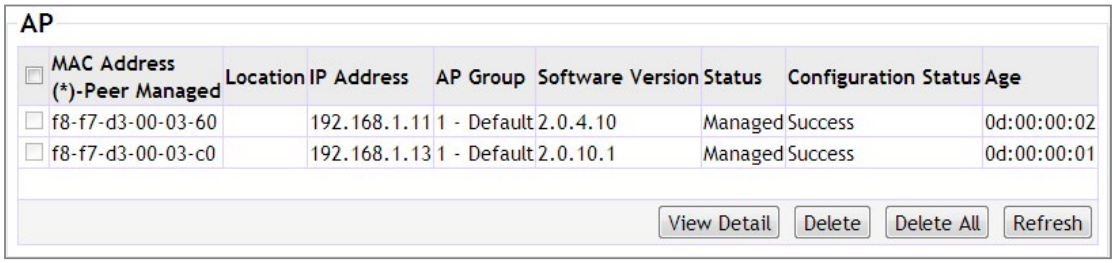
20.2 AP

Click **Monitor->AP** to open the **AP Monitor** page to monitor the basic AP information, AP detail, and the failure AP list. The user can delete the failed managed AP.



20.2.1 Basic AP information

Basic AP Information includes **MAC Address (*)-Peer Managed**, **Location, IP Address**, **AP Group**, **Software Version**, **Status**, **Configuration Status**, and **Age**.



Example:

1. Select the **Failed** Managed AP, and then click **Delete** to delete it.
2. Select **MAC Address (*)-Peer Managed**, and then click **Delete** to delete all failed managed APs.

20.2.2 AP detail

Click **View Detail** on the **Monitor->AP** page to view the AP detail that includes Managed AP Status, Radio Detail, Neighbor APs, Neighbor Clients, VAP, VAP TSPEC, and Distributed Tunneling Status. Click **View Detail** again, or click **Cancel** to exit the **AP Detail** page.

20.2.2.1 Managed AP status

From the Managed AP MAC Address list select the MAC address and view the corresponding AP status detail. The **Managed AP Status** includes IP Address, Managing AC, Status, Configuration Status, Authenticated Clients, CPU Usage, TSPEC Status, etc.

Managed AP Status

Managed AP Status

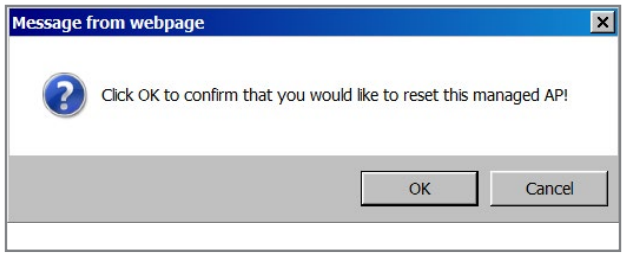
f8-f7-d3-00-03-60

IP Address	192.168.1.11	Managing AC	Local Switch
IP Subnet Mask	255.255.255.0	AC MAC Address	f8-f7-d3-00-03-f0
Status	Managed	AC IP Address	192.168.1.1
Software Version	2.0.4.10	AP Group	1 - Default
Code Download Status	Not Started	Discovery Reason	AC IP Configured
Configuration Status	Success	Protocol Version	2
Vendor ID	International Communications Corporation	Authenticated Clients	0
Hardware Type	22 - ARC2000MAP, Indoor Dual Band Radio 802.11N	System Up Time	0d:00:20:50
Serial Number	13150505	Age	0d:00:00:01
CPU Type	AR9344-533	CPU Usage(%-5s)	5
CPU Usage(%-30s)	8	CPU Usage(%-5min)	7
Memory Size Total(KB)	112672	Memory Size Used(KB)	23152

TSPEC Status

Type	Voice	Video
Number of Active Traffic Streams	0	0
Number of Traffic Stream Clients	0	0
Number of Traffic Stream Roaming Clients	0	0

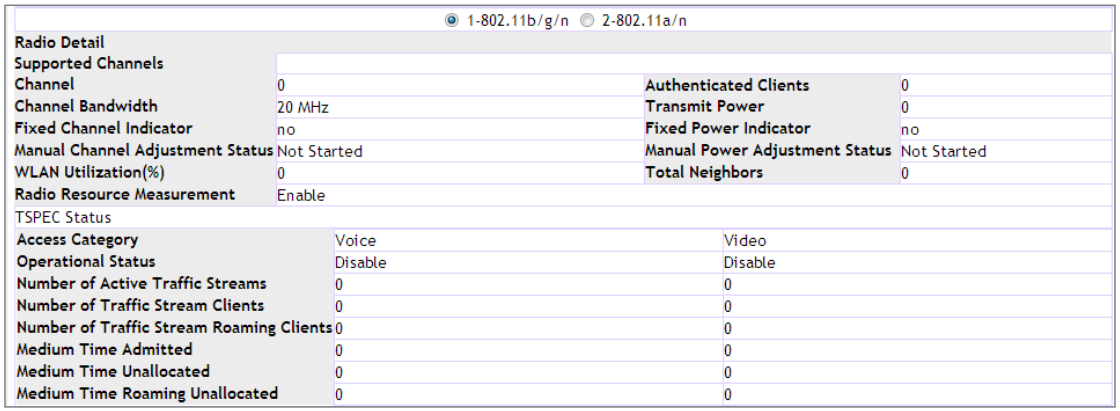
To reboot the AP, make the selection from the AP MAC Address list, select the corresponding MAC address and click **Reset**. The **Message from webpage** dialog box will appear. Click **OK** to complete the configuration reset.



20.2.2.2 Radio detail

Radio Detail includes Supported Channels, Channel, Authenticated Clients, Channel Bandwidth, Fixed Channel Indicator, Fixed Power Indicator, Manual Channel Adjustment Status, Manual Power Adjustment Status, WLAN Utilization (%), Total Neighbors, TSPEC Status, etc.

Select either **1-off** for Radio 1 or **2-802.11a/n** for Radio 2 to monitor their status, as shown in the following figure (Radio 1 detailed):



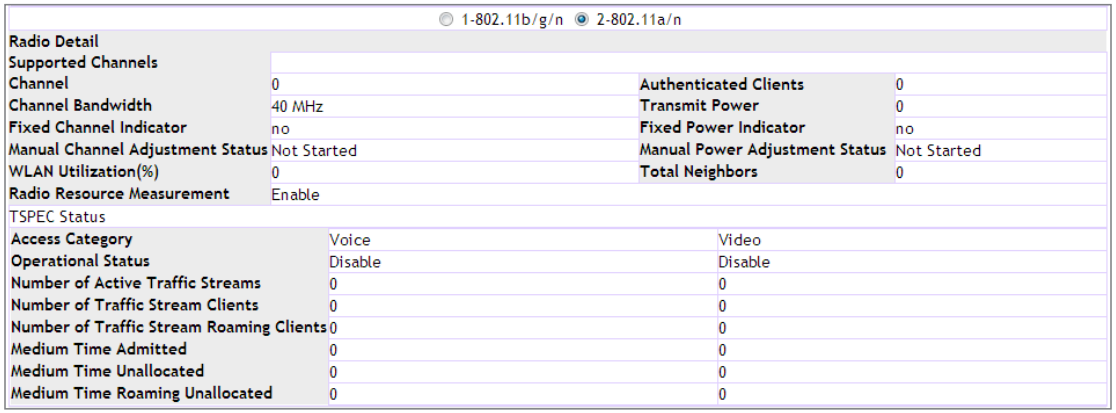
1-802.11b/g/n 2-802.11a/n

Radio Detail			
Supported Channels			
Channel	0	Authenticated Clients	0
Channel Bandwidth	20 MHz	Transmit Power	0
Fixed Channel Indicator	no	Fixed Power Indicator	no
Manual Channel Adjustment Status	Not Started	Manual Power Adjustment Status	Not Started
WLAN Utilization(%)	0	Total Neighbors	0
Radio Resource Measurement	Enable		

TSPEC Status

Access Category	Voice	Video
Operational Status	Disable	Disable
Number of Active Traffic Streams	0	0
Number of Traffic Stream Clients	0	0
Number of Traffic Stream Roaming Clients	0	0
Medium Time Admitted	0	0
Medium Time Unallocated	0	0
Medium Time Roaming Unallocated	0	0

If a dual band radio is being monitored, Radio 2 detail is shown as follows:



1-802.11b/g/n 2-802.11a/n

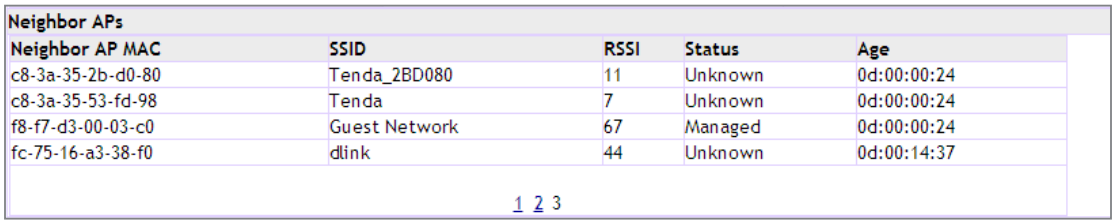
Radio Detail			
Supported Channels			
Channel	0	Authenticated Clients	0
Channel Bandwidth	40 MHz	Transmit Power	0
Fixed Channel Indicator	no	Fixed Power Indicator	no
Manual Channel Adjustment Status	Not Started	Manual Power Adjustment Status	Not Started
WLAN Utilization(%)	0	Total Neighbors	0
Radio Resource Measurement	Enable		

TSPEC Status

Access Category	Voice	Video
Operational Status	Disable	Disable
Number of Active Traffic Streams	0	0
Number of Traffic Stream Clients	0	0
Number of Traffic Stream Roaming Clients	0	0
Medium Time Admitted	0	0
Medium Time Unallocated	0	0
Medium Time Roaming Unallocated	0	0

20.2.2.3 Neighbor APs

APs can detect the surrounding RF in real time, including neighbor APs and neighbor clients. The neighbor APs' information is shown as follows:



Neighbor APs

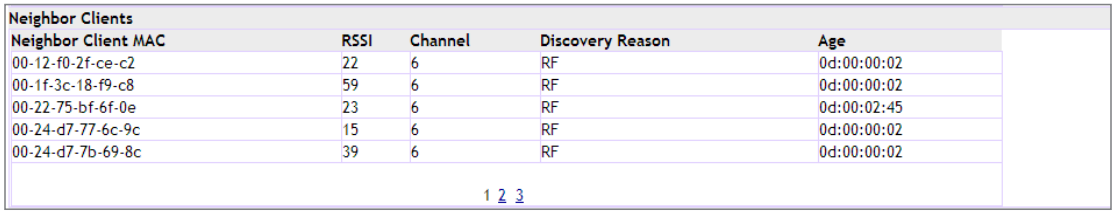
Neighbor AP MAC	SSID	RSSI	Status	Age
c8-3a-35-2b-d0-80	Tenda_2BD080	11	Unknown	0d:00:00:24
c8-3a-35-53-fd-98	Tenda	7	Unknown	0d:00:00:24
f8-f7-d3-00-03-c0	Guest Network	67	Managed	0d:00:00:24
fc-75-16-a3-38-f0	dlink	44	Unknown	0d:00:14:37

1 2 3

- Neighbor AP MAC – detected AP MAC
- SSID – SSID of AP network
- RSSI – received signal strength indication of AP
- Status – includes **Managed**, **Standalone (fat AP)**, **Unknown**, and **Rogue**
- Age – how long in terms of days, hours, minutes, and seconds that the AP has been detected

20.2.2.4 Neighbor clients

The Neighbor Clients' information is as follows:



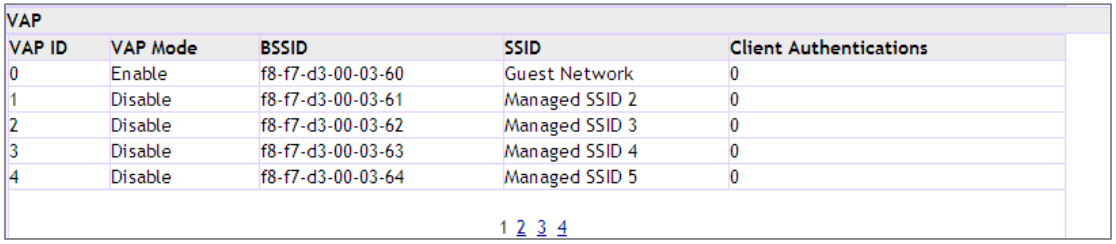
Neighbor Clients

Neighbor Client MAC	RSSI	Channel	Discovery Reason	Age
00-12-f0-2f-ce-c2	22	6	RF	0d:00:00:02
00-1f-3c-18-f9-c8	59	6	RF	0d:00:00:02
00-22-75-bf-6f-0e	23	6	RF	0d:00:02:45
00-24-d7-77-6c-9c	15	6	RF	0d:00:00:02
00-24-d7-7b-69-8c	39	6	RF	0d:00:00:02

1 2 3

20.2.2.5 VAP

VAP details include VAP ID, VAP Mode, BSSID, SSID, and Client Authentications, as shown in the following figure:



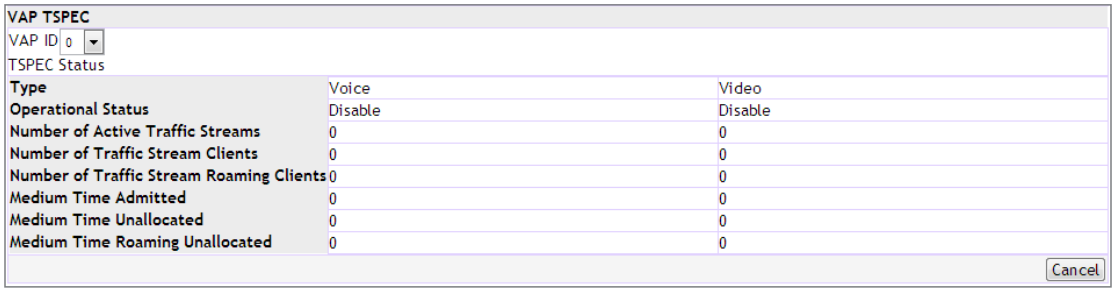
VAP

VAP ID	VAP Mode	BSSID	SSID	Client Authentications
0	Enable	f8-f7-d3-00-03-60	Guest Network	0
1	Disable	f8-f7-d3-00-03-61	Managed SSID 2	0
2	Disable	f8-f7-d3-00-03-62	Managed SSID 3	0
3	Disable	f8-f7-d3-00-03-63	Managed SSID 4	0
4	Disable	f8-f7-d3-00-03-64	Managed SSID 5	0

1 2 3 4

20.2.2.6 VAP TSPEC

Select the VAP ID list to view the corresponding TSPEC status of VAP as shown in the following figure:



VAP TSPEC

VAP ID 0

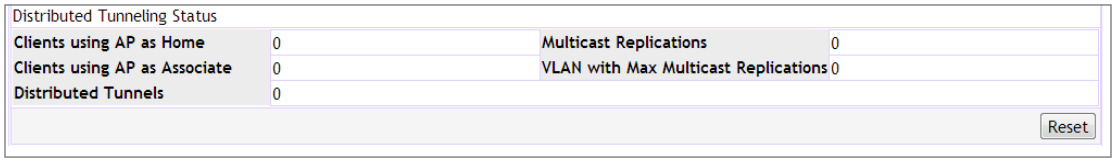
TSPEC Status

Type	Voice	Video
Operational Status	Disable	Disable
Number of Active Traffic Streams	0	0
Number of Traffic Stream Clients	0	0
Number of Traffic Stream Roaming Clients	0	0
Medium Time Admitted	0	0
Medium Time Unallocated	0	0
Medium Time Roaming Unallocated	0	0

Cancel

20.2.2.7 Distributed tunneling status

Distributed Tunneling Status includes Clients using AP as home, Multicast Replications, Clients using AP as Associate, VLAN with Max Multicast Replications, and Distributed Tunnels (including Home AP terminal and Association AP terminal).



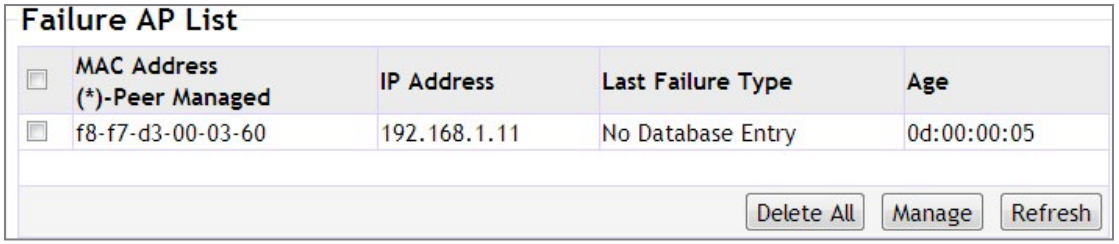
Distributed Tunneling Status

Clients using AP as Home	0	Multicast Replications	0
Clients using AP as Associate	0	VLAN with Max Multicast Replications	0
Distributed Tunnels	0		

Reset

20.2.3 Failure AP list

The **Failure AP List** shows the failed authentication AP details . If the Link1000ACS is the cluster controller, the failed authentication AP information of the other Link1000ACS in the cluster will also be shown. To distinguish, there is an asterisk before the failed authentication AP of non-local APs.

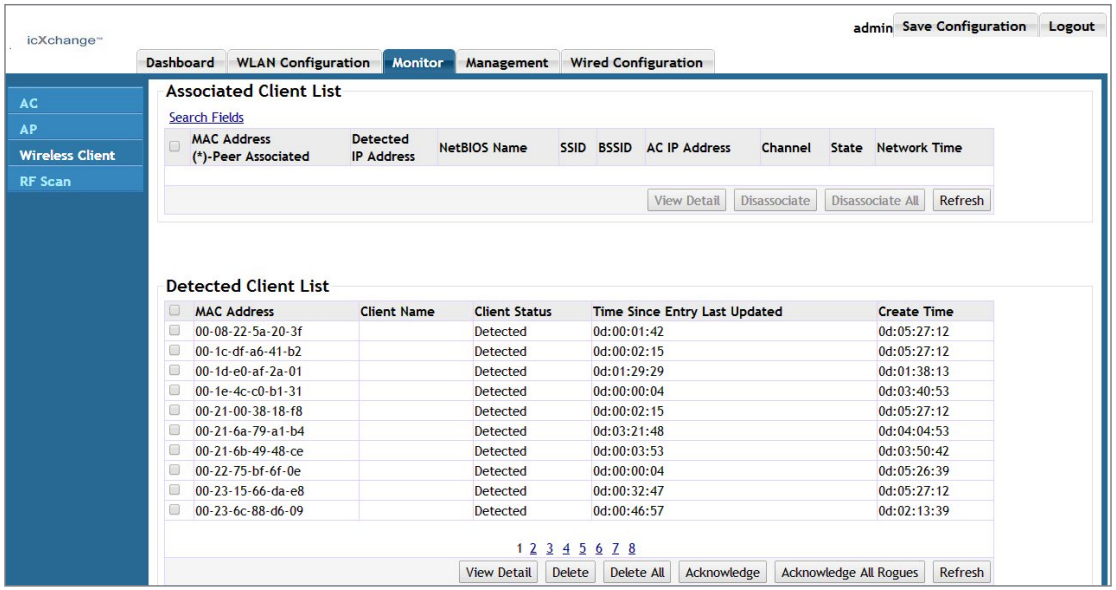


Click **Delete All** to delete the Failure AP List.

Select the Failure AP List, and then click **Managed**. The message box will appear. Click **OK**, and this AP will be configured as the effective managed AP with the default profile. It will be managed when discovered in future deployments.

20.3 Wireless client

Click **Monitor->Wireless Client** to configure the associated and detected clients' information.



20.3.1 Associated client list

The associated client list displays the information of the associated clients including:

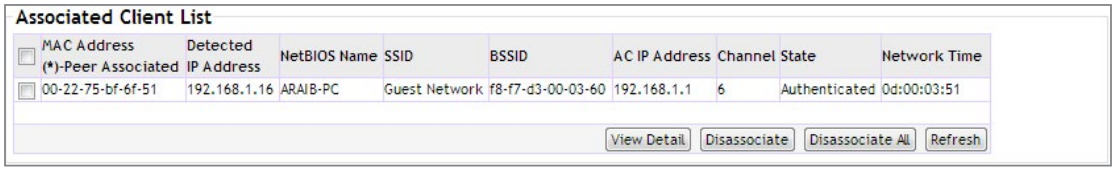
- MAC Address – the client's MAC address (the MAC address with asterisk is the address of the associated client on the peer switch)
- Detected IP Address – the IP address of the client
- NETBIOS Name – the name of the client under the NETBIOS protocol
- SSID – the network name
- BSSID – the MAC address of the associated VAP
- AC IP Address – the IP address of the managed AC

- Channel – the channel that the client uses to communicate with the AP
- State – the current authentication state of the client
- Network Time – the interval from the client connecting to the network to current

Click **View Detail** to view the associated clients' details, which are shown in the following section. Click **Disassociate** to disassociate the current selected client. Click **Disassociate All** to disassociate all clients. Click **Refresh** to refresh the list.

Example: Select the client to be disassociated, click **Disassociate**, and then click **Refresh**. This client will be disassociated.

Note: The disassociated client may become associated again automatically.

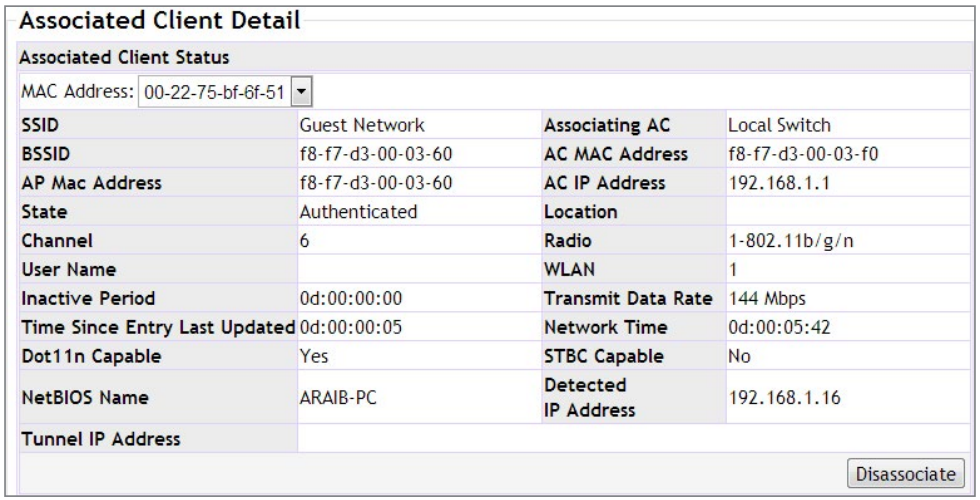


20.3.2 Associated client detail

Click **View Detail** to view the associated clients' details. Select the client in the drop-down list, and then click **View Detail**. Click **Cancel** to close the detail.

20.3.2.1 Associated client status

Click the **MAC Address** drop-down list and select a client to view **Associated Client Detail**.



Associated Client Detail

Associated Client Status

MAC Address: 00-22-75-bf-6f-51

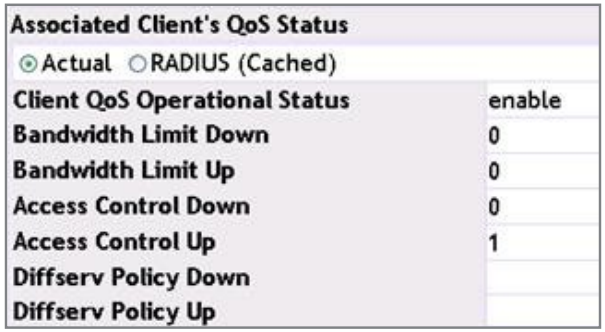
SSID	Guest Network	**Associating AC**	Local Switch
BSSID	f8-f7-d3-00-03-60	**AC MAC Address**	f8-f7-d3-00-03-f0
AP Mac Address	f8-f7-d3-00-03-60	**AC IP Address**	192.168.1.1
State	Authenticated	**Location**	
Channel	6	**Radio**	1-802.11b/g/n
User Name		**WLAN**	1
Inactive Period	0d:00:00:00	**Transmit Data Rate**	144 Mbps
Time Since Entry Last Updated	0d:00:00:05	**Network Time**	0d:00:05:42
Dot11n Capable	Yes	**STBC Capable**	No
NetBIOS Name	ARAIB-PC	**Detected IP Address**	192.168.1.16
Tunnel IP Address			

Disassociate

Click **Disassociate** to disassociate the client.

20.3.2.2 Associated client's QoS status

If the client is associated with the configured QoS network, the client's QoS status can be viewed as follows:



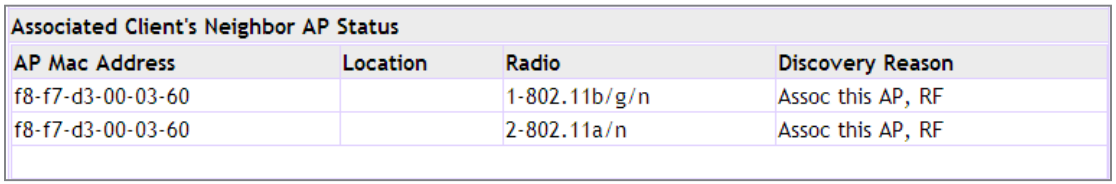
Associated Client's QoS Status

◉ Actual ○ RADIUS (Cached)

Client QoS Operational Status	enable
Bandwidth Limit Down	0
Bandwidth Limit Up	0
Access Control Down	0
Access Control Up	1
Diffserv Policy Down	
Diffserv Policy Up	

20.3.2.3 Associated client's neighbor AP status

The **Associated Client's Neighbor AP** is the neighbor AP that the client scanned including the associated AP. This client only scanned the AP associated with itself but did not scan the other AP:

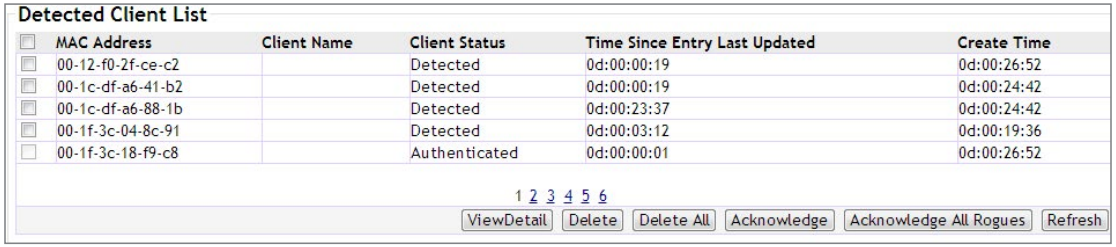


Associated Client's Neighbor AP Status

AP Mac Address	Location	Radio	Discovery Reason
f8-f7-d3-00-03-60		1-802.11b/g/n	Assoc this AP, RF
f8-f7-d3-00-03-60		2-802.11a/n	Assoc this AP, RF

20.3.3 Detected client list

The **Detected Client List** includes the client associated with AP and the scanned client. The detected client list is as follows:



Detected Client List

MAC Address	Client Name	Client Status	Time Since Entry Last Updated	Create Time
00-12-f0-2f-ce-c2		Detected	0d:00:00:19	0d:00:26:52
00-1c-df-a6-41-b2		Detected	0d:00:00:19	0d:00:24:42
00-1c-df-a6-88-1b		Detected	0d:00:23:37	0d:00:24:42
00-1f-3c-04-8c-91		Detected	0d:00:03:12	0d:00:19:36
00-1f-3c-18-f9-c8		Authenticated	0d:00:00:01	0d:00:26:52

1 2 3 4 5 6

ViewDetail | Delete | Delete All | Acknowledge | Acknowledge All Rogues | Refresh

Select one client, and then click **View Detail** to view the client detail status. Select one client, and then click **Delete** to delete this client. Click **Delete All** to delete all detected clients.

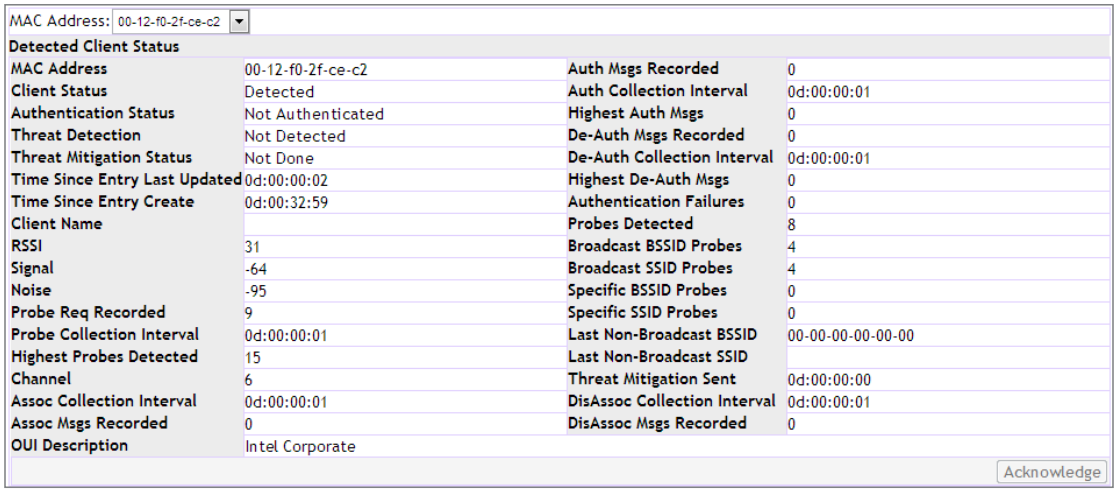
Note: The associated clients will not be deleted. Select the rogue client, and click **Acknowledge** to clear this rogue client; click **Acknowledge All Rogues** to clear all rogue clients.

20.3.4 Detected client detail

Click **View Detail** to view the detected client detail.

20.3.4.1 Detected client status

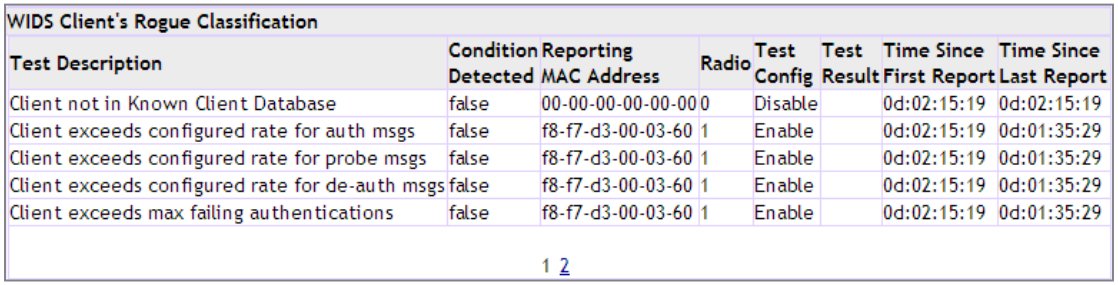
Select the client in the **MAC Address** drop-down list to view **Detected Client Status**.



If this client is rogue, click **Acknowledge** to clear this client.

20.3.4.2 WIDS client's rogue classification

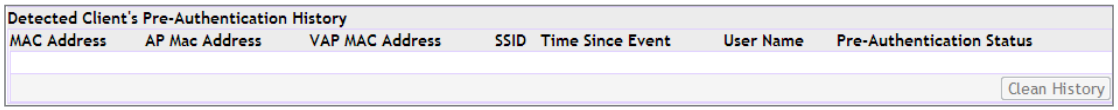
For the selected clients, **WIDS Client's Rogue Classification** can display the rogue classification status of this client, as shown in the following figure:


WIDS Client's Rogue Classification
Test Description | Condition Detected | Reporting MAC Address | Radio | Test Config | Test Result | Time Since First Report | Time Since Last Report
Client not in Known Client Database | false | 00-00-00-00-00-00 | 0 | Disable | | 0d:02:15:19 | 0d:02:15:19
Client exceeds configured rate for auth msgs | false | f8-f7-d3-00-03-60 | 1 | Enable | | 0d:02:15:19 | 0d:01:35:29
Client exceeds configured rate for probe msgs | false | f8-f7-d3-00-03-60 | 1 | Enable | | 0d:02:15:19 | 0d:01:35:29
Client exceeds configured rate for de-auth msgs | false | f8-f7-d3-00-03-60 | 1 | Enable | | 0d:02:15:19 | 0d:01:35:29
Client exceeds max failing authentications | false | f8-f7-d3-00-03-60 | 1 | Enable | | 0d:02:15:19 | 0d:01:35:29
1 2

- Test Description – detail WIDS client's rogue classification.
- Condition Detected – **false** indicates that this item does not meet the rogue detection condition; **true** indicates that this rogue detection is founded and it is the rogue client.
- Reporting MAC Address – indicates the AP that reports the information. If the MAC address is all 0s, no AP reports the client's test item.

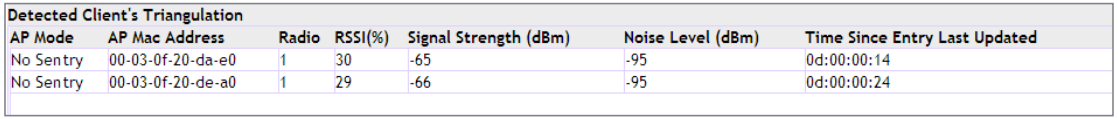
20.3.4.3 Detected client's pre-authentication history

If the detected client has the authentication history, it displays the information as follows:



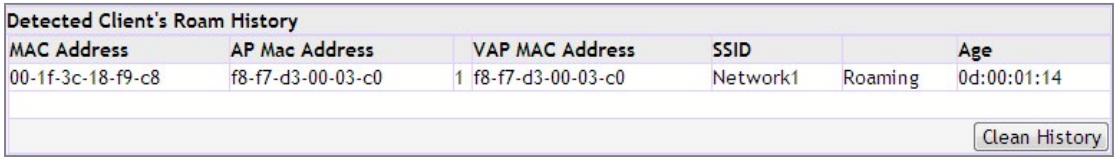
20.3.4.4 Detected client's triangulation

The client's approximate location can be detected by the access point (AP) by relative signal strength. The table of the AP's signal strength is reported as follows:



20.3.4.5 Detected client's roam history

The **Detected Client's Roam History** can display the roam history of the client that is being associated or that had been associated but is not associated now. The following figure shows the roam history of the client whose MAC is 00-1f-3c-18-f9-c8:



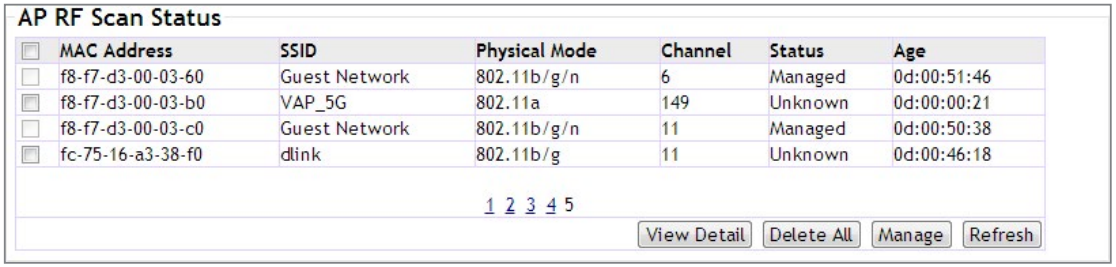
The AP MAC is one of the current APs that the client has roamed to.

20.4 RF scan

Click **Monitor->RF Scan** to open the **RF Scan** page. It includes AP RF scan status and client dynamic blacklist.

20.4.1 AP RF scan status

AP RF Scan Status shows all the APs' scanned information:



The AP RF scan status list describes all the APs' statuses scanned in the wireless network. The AP monitors the RF environment including client and AP information. It will send the monitored information periodically to the associated AC.

- MAC Address – the MAC address of the scanned AP
- SSID – the network SSID sent by the scanned AP
- Physical Mode – the detected radio mode of the scanned AP
- Channel – the detecte channel of the scanned AP
- Status – the status of the scanned AP including **Unknown**, **Managed**, and **Rogue**
- Age – the interval from the last scanning to current

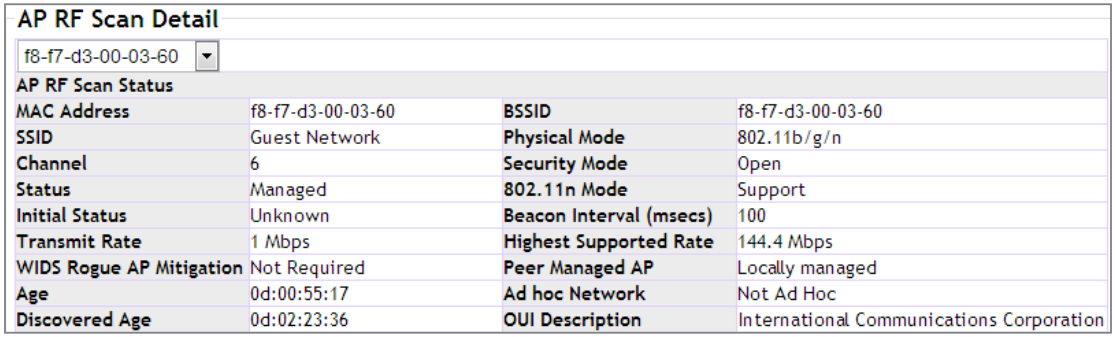
Click **View Detail** to view the RF scan status of one AP. Click **Delete All** to delete all the scanned APs. Click **Manage** to add the selected AP into the AP database. Click **Refresh** to refresh the scan information.

20.4.2 AP RF scan detail

Click **View Detail** in the AP RF scan status to open the detail information.

20.4.2.1 AP RF scan status

Select the AP in the **AP RF Scan Detail** drop-down list to view detailed information.



AP RF Scan Detail

f8-f7-d3-00-03-60

AP RF Scan Status			
MAC Address	f8-f7-d3-00-03-60	**BSSID**	f8-f7-d3-00-03-60
SSID	Guest Network	**Physical Mode**	802.11b/g/n
Channel	6	**Security Mode**	Open
Status	Managed	**802.11n Mode**	Support
Initial Status	Unknown	**Beacon Interval (msecs)**	100
Transmit Rate	1 Mbps	**Highest Supported Rate**	144.4 Mbps
WIDS Rogue AP Mitigation	Not Required	**Peer Managed AP**	Locally managed
Age	0d:00:55:17	**Ad hoc Network**	Not Ad Hoc
Discovered Age	0d:02:23:36	**OUI Description**	International Communications Corporation

- MAC Address – the MAC address of the scanned AP
- BSSID – the MAC address of the associated VAP
- SSID – name of the network in use by the AP
- Physical Mode – the 802.11 mode in use by the AP
- Channel – the transmission channel in use by the AP
- Security Mode – the security scheme used by the AP. Includes **Open**, **WEP**, and **WPA** authentication
- Status – if the AP is managed or failed on the Link1000ACS
- 802.11n Mode – the current transmission mode of the AP
- Initial Status – the status when the access point was initially detected
- Beacon Interval – the current beacon interval assigned in the AP configuration
- Transmit Rate – the current transmission rate of the AP
- Highest Supported Rate – the highest supported transmission rate as assigned in the AP configuration
- WIDS Rogue AP Mitigation – shows if the mitigation for the rogue AP is enabled/disabled
- Peer Managed AP – the peer managed AP as assigned in the AP configuration
- Age – the interval from the last scanning and reporting to current

- Ad hoc Network – reports if the network is ad hoc
- Discovered Age – the interval from the first scanning to current
- OUI Description – the name of the AP's manufacturer

20.4.2.2 AP triangulation status

AP Triangulation Status shows the neighbor AP information for the AP location. The location information includes three radios that are not in sentry mode and three radios that are in sentry mode. The AP triangulation status is as follows:

AP Triangulation Status

AP Mode	AP Mac Address	Radio	RSSI(%)	Signal Strength (dBm)	Noise Level (dBm)	Age
No Sentry	f8-f7-d3-00-03-c0	1	0	-95	-95	0d:00:55:17

20.4.2.3 WIDS AP rogue classification

The scanned AP can determine if the AP is rogue AP through WIDS. The Rogue Classification is as follows:

WIDS AP Rogue Classification

Status Managed

Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Administrator configured rogue AP	false	00-00-00-00-00-00	0	Enable		0d:00:00:00	0d:00:00:00
Managed SSID from an unknown AP	false	00-00-00-00-00-00	0	Disable		0d:00:00:00	0d:00:00:00
Managed SSID from a fake managed AP	false	00-00-00-00-00-00	0	Disable		0d:00:00:00	0d:00:00:00
AP without an SSID	false	00-00-00-00-00-00	0	Disable		0d:00:00:00	0d:00:00:00
Fake managed AP on an invalid channel	false	00-00-00-00-00-00	0	Disable		0d:00:00:00	0d:00:00:00

1 2 3

If the scanned AP confirms any of the items, it will determine that it is a rogue AP.

20.4.3 Client dynamic blacklist

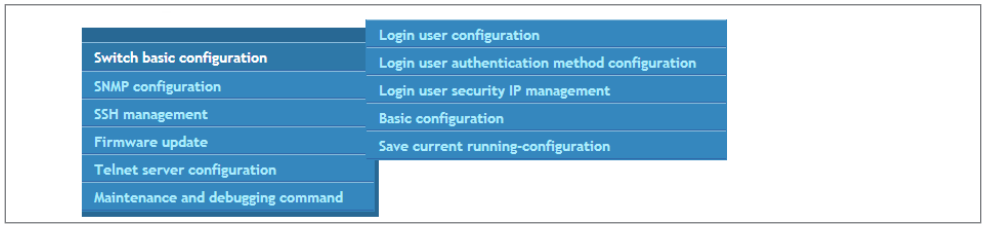
The wireless RF can report the client as the dynamic blacklist through the **Client Dynamic Blacklist** conditions. The scanned dynamic blacklist is as follows:

Click **Delete** to delete the selected client. Click **Delete All** to delete the entire Client Dynamic Blacklist.

Chapter 21: Management

21.1 Basic configuration

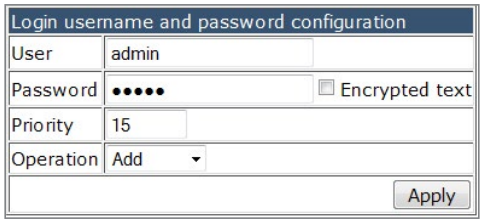
Click **Management->Switch Basic Configuration** to configure **Login user configuration**, **Login user authentication method configuration**, **Login user security IP management**, and **Basic Configuration**. Users can also **Save the current running-configuration**, set the AC to factory default and warm reboot the AC with or without saving the current configuration.



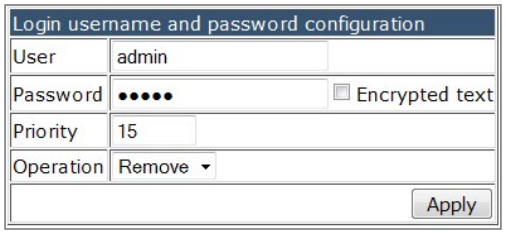
21.1.1 Login user configuration

Click **Management->Switch basic configuration->Login user configuration** to add or delete the user information.

Example: Configure a user with a Name and Password both as **admin** and with Priority of **15**.



Click **Apply**, and the added user information will be displayed as follows:



- User – the appointed username
- Password – configures the appointed password
- Encrypted text – selects if the input password is shown in plain text or encrypted
- Priority – only the user whose priority is 15 can log in to the **WEB Management** page
- Operation – includes **Add** and **Remove**

21.1.2 Login user authentication method configuration

Click **Management->Switch Basic Configuration->Login user authentication method configuration** to configure the VTY (the login methods of Telnet and SSH), Web, Console methods and the login user authentication method and priority.

The Login methods include **Console**, **VTY** (including Telnet and SSH),and **Web**. The Authentication method must be **Local**, **Radius**, or **Tacacs**. Local is to use the local database for authentication; Radius is to use the Radius remote authentication server for authentication; tacacs is to use the Tacacs+ remote authentication server for authentication. There is no need to authenticate in console method as default; the Authentication methods of **VTY** and **Web** are **Local** authentication by default.

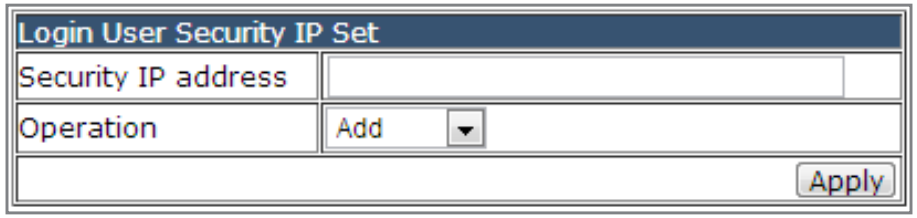
Example: Configure a user who uses the Radius remote authentication server for authentication with Telnet and SSH.

Note: The corresponding user authentication method can be configured for Console, VTY, and Web, respectively. The authentication method can be selected as any combination of **Local**, **Radius**, and **Tacacs**. When adopting the combination authentication methods, the priority of authentication method 1 is highest and then falls in descending order. If the authentication method with higher priority is successful, the user will be allowed to log in with those credentials and the subsequent authentication methods will be ignored.

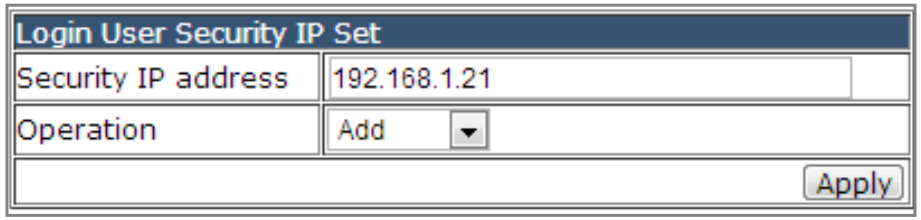
21.1.3 Login user security IP management

Click **Management->Switch Basic Configuration->Login User Security IP Management** to configure the security IP address used by Telnet and HTTP methods.

Prior to configuring the security IP address, the IP addresses for logging into the switch is not limited. After configuring, only a user originating from a security IP address can log in to the switch for configuration. Up to 32 security IP addresses can be configured.



Example: Type **192.168.1.21** as the Security IP address, and click **Apply** to complete the configuration.

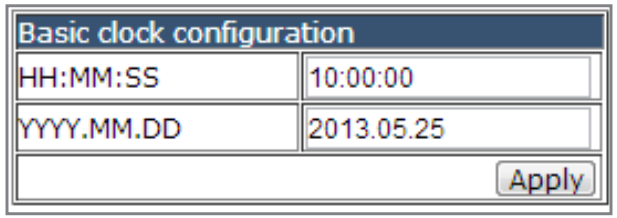


21.1.4 Basic configuration

Click **Management->Switch Basic Configuration->Basic Configuration** to configure the clock, switch name, and exec timeout (auto-timeout for management).

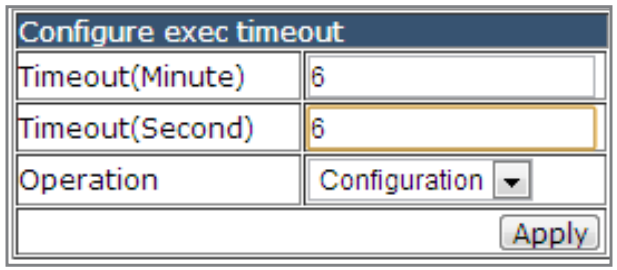
1. Basic clock configuration – configures the system date and time.

Example: Type the HH:MM:SS as **10:00:00**, and configure the YYYY.MM.DD as **2013.05.25**. Click **Apply** to complete the configuration.



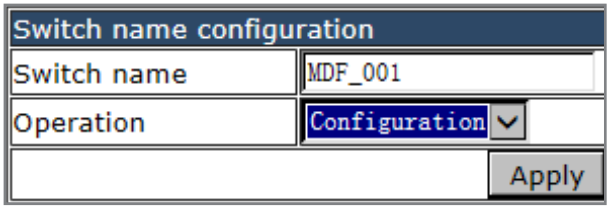
2. Configure exec timeout.

Example: Type the Timeout (Minute) as **6** and the Timeout (Second) as **6**, and then click **Apply** to configure a six minute and six second timeout for exec commands.



3. Switch name configuration.

Example: Type the Switch Name as **Switch**, and click **Apply** to configure a switch name.



- Operation – **Configuration** or **Default**

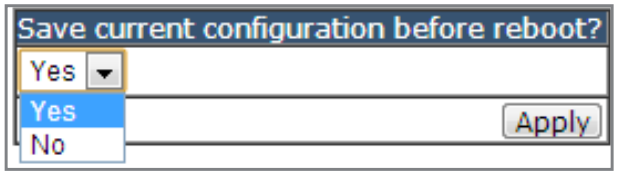
21.1.5 Save current running-configuration

Click **Management->Switch Basic Configuration->Save current running-configuration** to save the current configuration.

1. Save current running-configuration – click **Apply** to save the current configuration.

The **Save current running-configuration** message will display as follows:

2. Save current configuration before reboot? – select **Yes** or **No**. Click **Apply**.

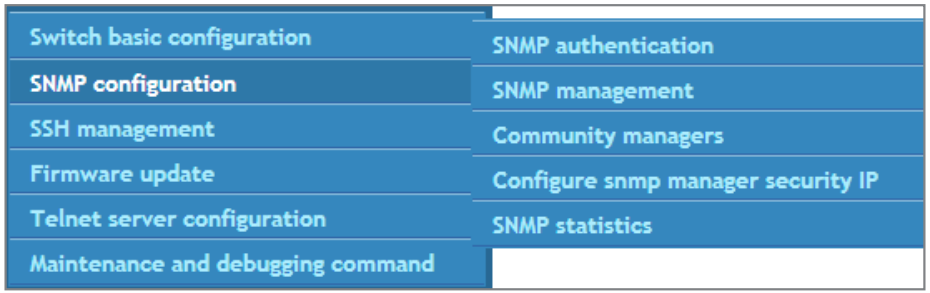


3. Reboot with the default configuration – click **Apply** to clear all the current configurations in the switch and restart the switch to factory default.

21.2 SNMP configuration

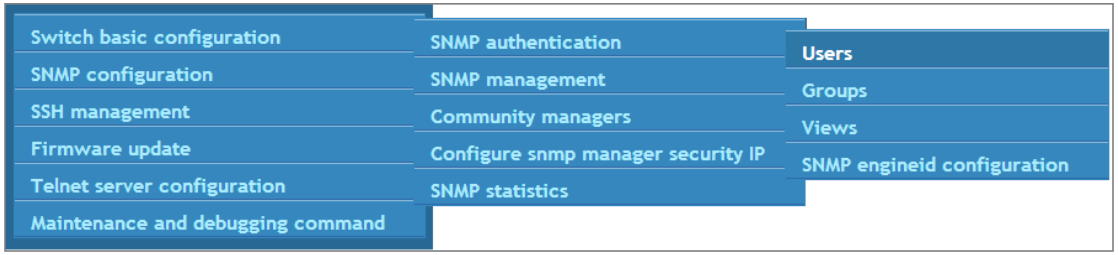
Click **Management->SNMP Configuration** to configure the SNMP function.

Note: Prior to configuration, SNMP must be enabled. Configure the **SNMP management** as **Open**, and then click **Apply**.



21.2.1 SNMP Authentication

Click **Management->SNMP Configuration->SNMP Authentication** to configure the SNMPv3 including Users, Groups, Views, and SNMP engineid configuration. The figure is as follows:

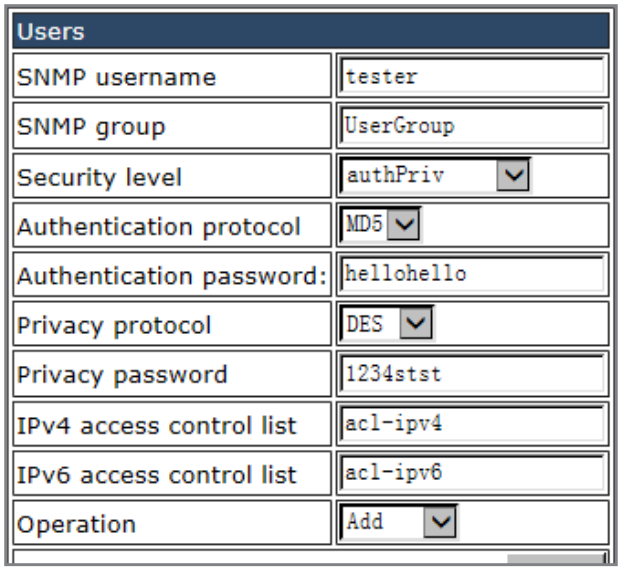


21.2.1.1 Users

Click **Management->SNMP Configuration->SNMP Authentication->Users** to add or delete SNMPv3 users.

- SNMP username – the username; range is from 1 to 32 characters
- SNMP group – the group name that the user belongs to; range is from 1 to 32 characters
- Security level – the encryption level of the current user: **noAuthNoPriv** for no authentication and no privacy; **AuthNoPriv** for authentication but no privacy; **AuthPriv** for authentication and privacy
- Authentication protocol – configures the used algorithm: **MD5** or **SHA**
- Authentication password – the authentication password of the current user; range is from 8 to 32 characters
- Privacy protocol – uses the DES for packet privacy. This can only be configured when the security level is selected as **AuthPriv**
- Privacy Password – password as configured on SNMP authorization server
- IPv4 access control list – control list defined in **Wired Configuration->ACL Configuration->Name ACL**
- IPv6 access control list – control list defined in **Wired Configuration->IPv6 ACL Configuration->IPv6 name access-list configuration**
- Operation – includes **Add** or **Delete**

Example: Type the SNMP username as **tester** and the SNMP group as **UserGroup**. Select the Security level as **authPriv** and the Authentication protocol as **MD5**. Type the Authentication password as **hellohello**. Select the Privacy protocol as **DES** and select the operation as **Add**. Click **Apply**.

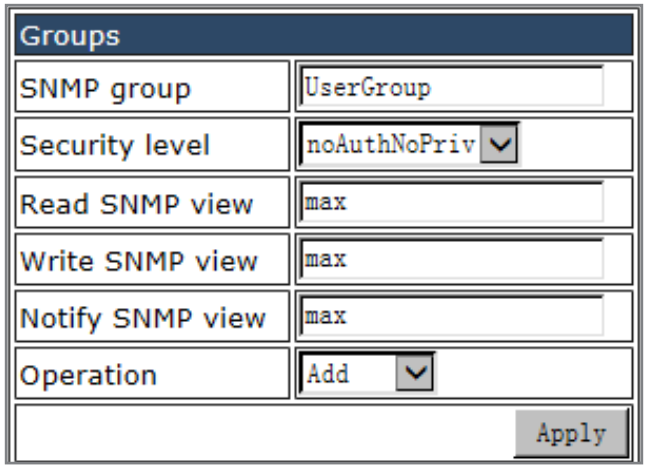


21.2.1.2 Groups

Click **Management->SNMP Configuration->SNMP Authentication->Groups** to add or delete SNMPv3 groups.

- SNMP group – the user group name of SNMP; range is from 1 to 32 characters
- Security level – the security level of the group: **noAuthNoPriv** is no authentication and no privacy; **AuthNoPriv** is authentication but no privacy; **AuthPriv** is authentication and privacy
- Read SNMP view – configures the SNMP view (community) name with read permission
- Write SNMP view – configures the SNMP view (community) name with write permission
- Notify SNMP view – configures the SNMP view (community) name with notify permission
- Operation – includes **Add** or **Delete**

Example: Type the SNMP group as **UserGroup**. Select the Security level as **authPriv.** Select **max** for the Read SNMP view, Read SNMP view, and NotifySNMP view options. Select the operation as **Add**. Click **Apply**.

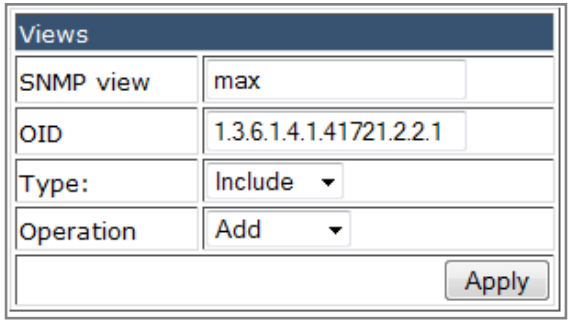


21.2.1.3 Views

Click **Management->SNMP Configuration->SNMP Authentication->Views** to add or delete SNMPv3 views.

- SNMP view – configures the view (community) name; range is from 1 to 32 characters
- OID – the OID or the corresponding node name; range is from 1 to 255 characters
- Type – configures the **Include**/**Exclude**
- Operation – includes **Add** or **Delete**

Example: Type the SNMP view as **max** and the OID as **1.3.6.1.4.1.41721.2.2.1**. Select the type as **Include** and the Operation as **Add**. Click **Apply**.

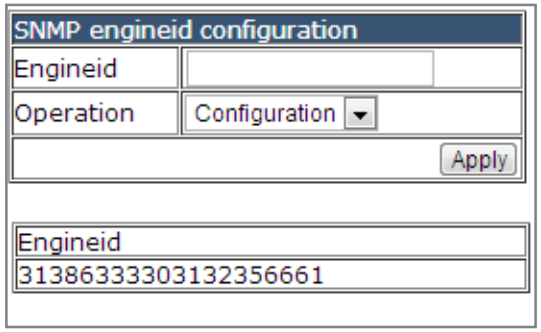


21.2.1.4 SNMP engineid configuration

Click **Management->SNMP Configuration->SNMP authentication-> SNMP engineid configuration** to configure the engine id.

- Engineid – the engine id; the range is from 1 to 32 hex characters
- Operation – **Configuration** or **Default**

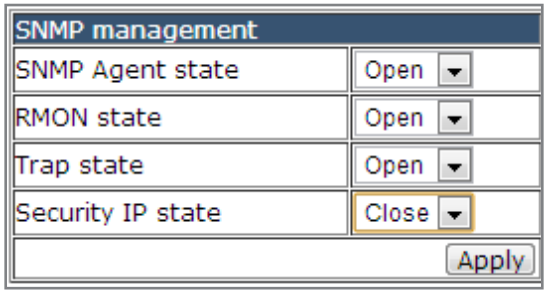
Example: Type the Engineid as **18c30125fa**, and select the Operation as **Configuration**. Click **Apply** to complete the engine ID of 31386333303132356661 as follows:



21.2.2 SNMP management

Click **Management->SNMP Configuration->SNMP management** to configure the SNMP Agent state, RMON state, Trap state, and Security IP state.

Example: Select the SNMP Agent state as **Open**, the RMON state as **Open**, the Trap state as **Open**, and the Security IP state as **Close**. Click **Apply**.



- SNMP Agent state – open or close the SNMP agent function of the switch
- RMON state – open or close the RMON function of the switch
- Trap State – open or close the function that the device receives the Trap information
- SecurityIP State – open or close the security IP address checking function of the NMS management station

21.2.3 Community managers

Click **Management->SNMP Configuration->Community Managers** to configure the community string and Trap manager.

1. Community managers – configure the community string and access priority
   - Community string (1 to 255 characters) – configures the community string
   - Access priority – includes **Read only** and **Read and Write**

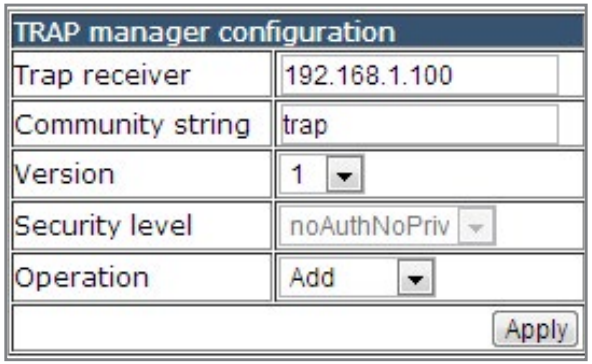
Example: Type the Community string as **public**, and select the Access priority as **Read only**. Click **Apply** to complete the configuration as follows:

2. Trap manager configuration

Click **Management->SNMP Configuration->community managers** to configure the community string and the IP address that receives the SNMP trap message.

- Trap receiver – the IP address that receives the trap message
- Community string (1 to 255 characters) – used to receive the trap message
- Version – **1**, **2** or **3**
- Security level – If version is equal to 3; **noAuthNoPriv**, **authNoPriv** or **authPriv**
- Operation – **Add** or **Remove**

Example: Type the Trap receiver as **192.168.1.100** Community string as **trap**. Click **Apply** to complete the configuration as follows:

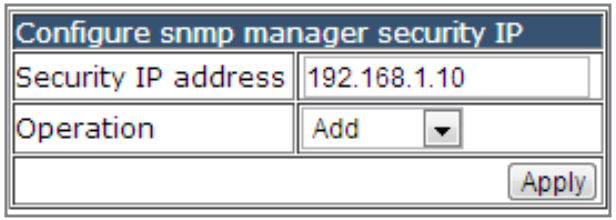


21.2.4 Configure SNMP manager security IP

Click **Management->SNMP Configuration->configure snmp manager security IP** to configure the security IP that allows access to the switch.

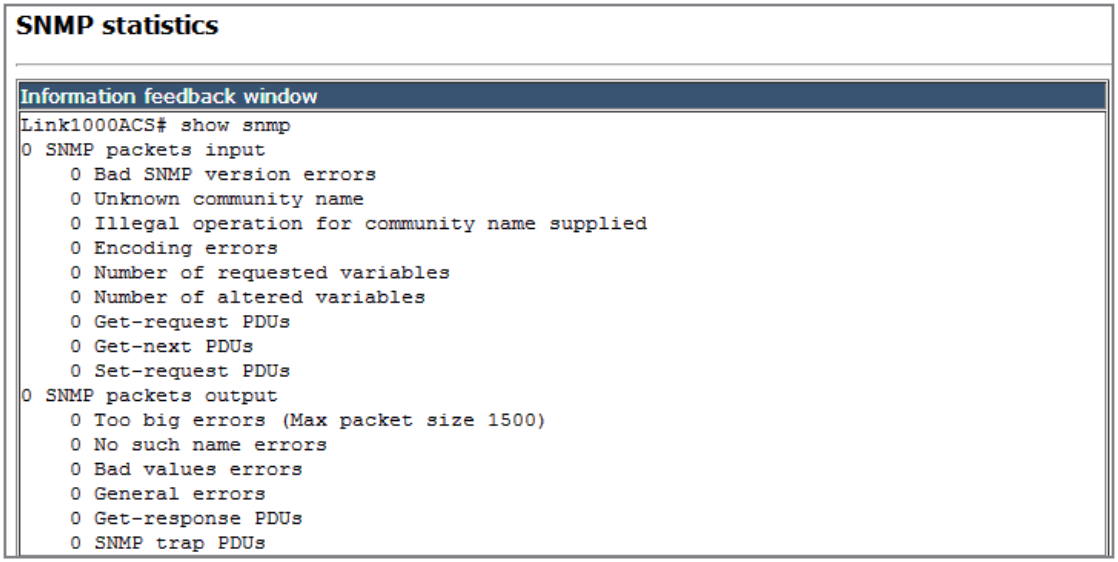
- Security IP address – the security IP address of NMS
- Operation – **Add** or **Remove**

Example: Type the Security IP address as **192.168.1.10** and then click **Apply** to complete the configuration as follows:



21.2.5 SNMP Statistics

Click **Management->SNMP Configuration->SNMP Statistics** to display the SNMP statistics.


SNMP statistics
Information feedback window
Link1000ACS# show snmp
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors (Max packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs

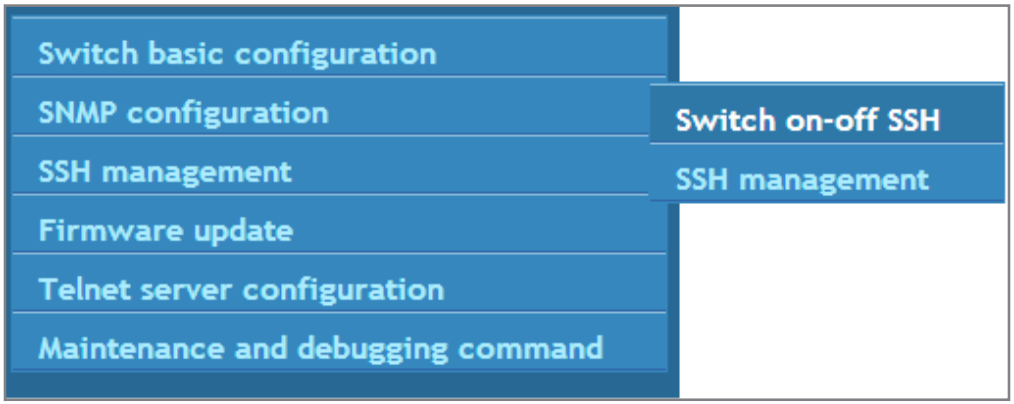
21.3 SSH management

Secure Shell (SSH) connections use a trusted SSL certificate for user logon to the web GUI interfaces. Browsers, such as Internet Explorer®, Firefox®, Safari® and Chrome™, come preinstalled with a predetermined set of root certificates. These certificates serve as trusted third parties and work instantly to provide seamless usability. The icXchange® solution accepts root SSL certificates from all browsers for a secure and encrypted https login. Users are not allowed to introduce their own certificates, thereby reducing the risk of unauthorized system access.

For any configurations discussed in the following subsections, **SSH** must be started as described in this section. If **SSH** is not started, the user may receive the message to "**Start SSH first before continuing the requested configuration**".

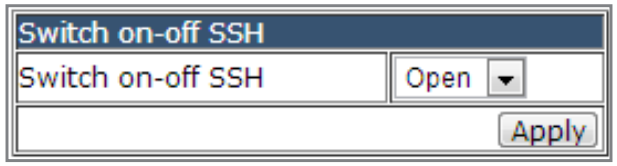
Click **Management->SSH management** to configure the SSH function.

Note: Enable the SSH prior to configuring. Select Switch on-off SSH as **Open**, and then click **Apply**.



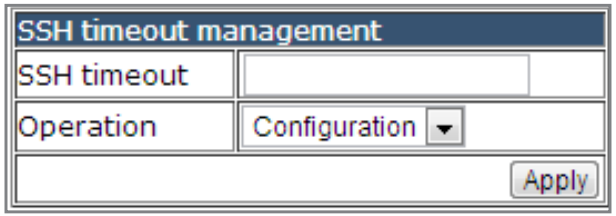
21.3.1 Switch on-off SSH

Click **Management->SSH management->Switch on-off SSH** to open or close the SSH function.

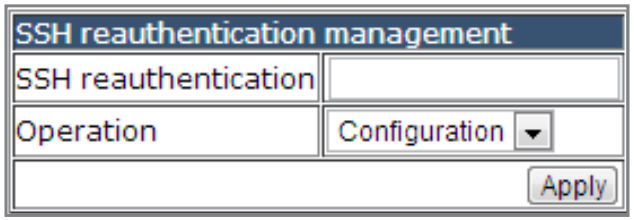


21.3.2 SSH management

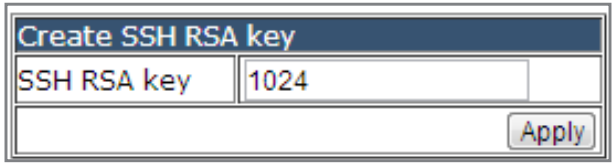
Click **Management->SSH management->SSH management** to configure SSH timeout management and SSH reauthentication management and to create SSH RSA key.



SSH timeout management – configures SSH timeout management; the range is from 10 to 600 seconds, and the default value is 180 seconds.



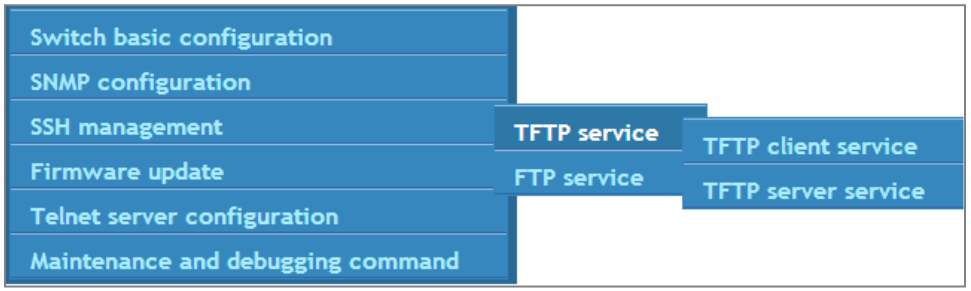
SSH reauthentication management – configures SSH reauthentication management; the range is from 1 to 10, and the default value is 3.



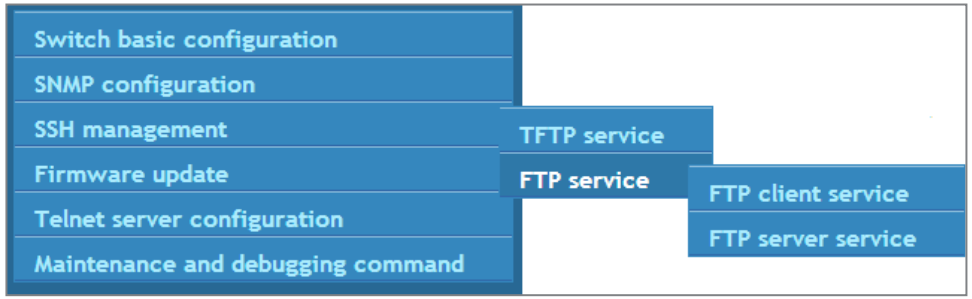
SSH RSA key – the algorithm for the host key; the range is from 768 to 2048, and the default value is 1024.

21.4 Firmware update

Click **Manage->Firmware update** to upgrade the switch by using TFTP or FTP service as shown in the following:



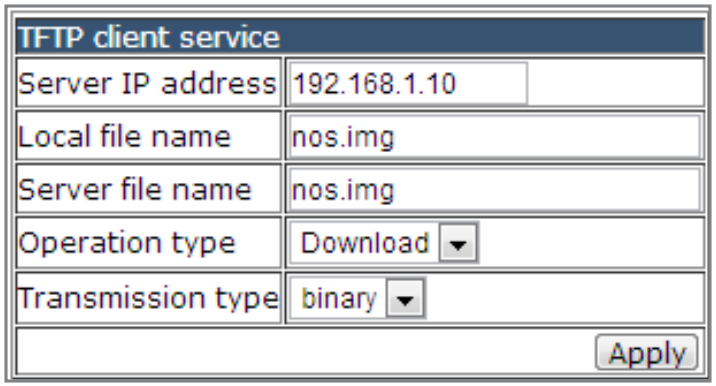
1. TFTP service includes:
   - TFTP client service – configures the TFTP client
   - TFTP server service – configures the TFTP server



2. FTP service includes:
   - FTP client service – configures the FTP client
   - FTP server service – configures the FTP server

21.4.1 TFTP client service

Click **Manage->Firmware update->TFTP service->TFTP client service** to open the configuration page:



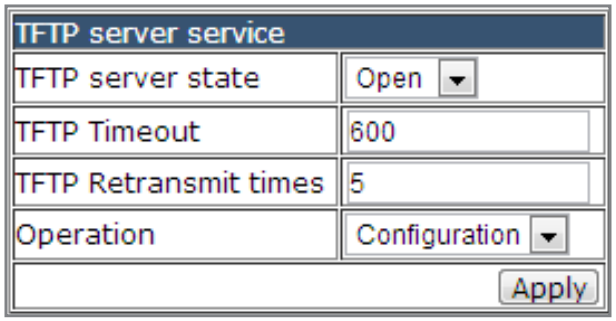
- Server IP address – the IP address of the TFTP server
- Local file name – destination file name; the range is from 1 to 100 characters
- Server file name – source file name; the range is from 1 to 100 characters
- Operation type – includes **Upload** and **Download**
- Transmission type – **ascii** uses ASCII to transmit the file; **binary** uses binary to transmit the file

Click **Apply**.

Note: The firmware upgrade process may take up to 15 minutes after loading the files onto the controller. After copying over the firmware image files to the controller, users should allow up to 15 minutes for the controller to complete the upgrade process prior to performing a reboot of the controller.

21.4.2 TFTP server service

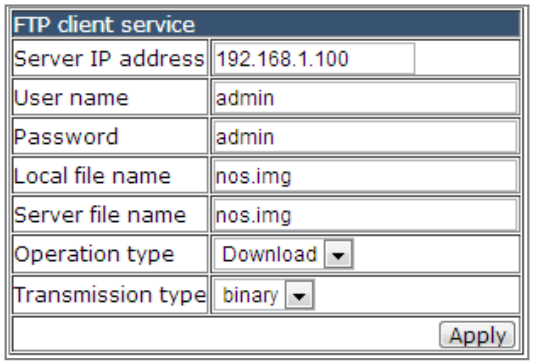
Click **Manage->Firmware update->TFTP service->TFTP server service** to open the configuration page.



- TFTP server state – the server state; includes **Open** and **Close**
- TFTP timeout – the timeout
- TFTP retransmit times – the times of retransmission
- Operation - **Configuration** or **Default**

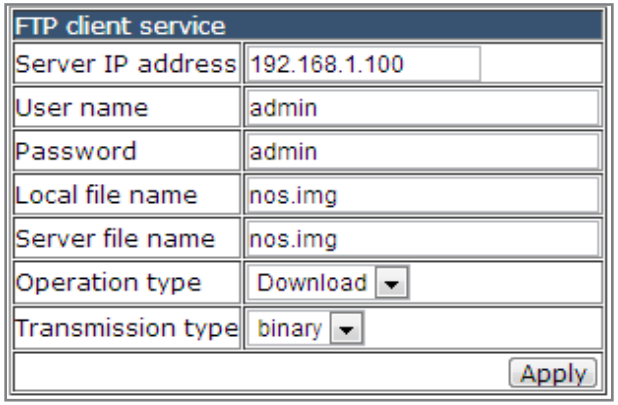
21.4.3 FTP client service

Click **Manage->firmware update->FTP service->FTP client service** to open the configuration page.



- Server IP address – the IP address of the FTPserver
- User name – the user name; range is from 1 to 100 characters
- Password – the appointed password; ranges from 1 to 100 characters
- Local file name – destination file name; range is from 1 to 100 characters
- Server file name – source file name; range is from 1 to 100 characters
- Operation type – includes **Upload** and **Download**
- Transmission type – **ascii** uses ASCII to transmit the file; **binary** uses binary to transmit the file

Example: Retrieve the system file whose local file name is **nos.img** and server file name is **nos.img** from the IP address of **192.168.1.100** (from the FTP server). The FTP user name and password are **admin**. Click **Apply**. The configuration is as follows:



21.4.4 FTP server service

Click **Manage->Firmware update->FTP service->FTP server service** to open the configuration page. It includes the FTP server service and FTP user name, as well as password setting.

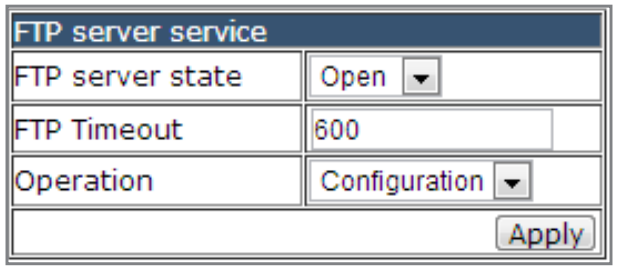
The glossary in FTP server service is below:

- FTP server state – the server state, which includes **Open** and **Close**
- FTP Timeout – range is from 5 to 3600 seconds
- Operation – includes **Configuration** and **Default**

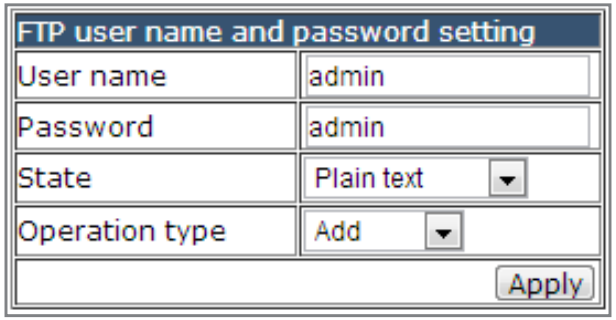
The glossary in FTP user name and password setting is as follows:

- User name – the user name; range is from 1 to 32 characters
- Password – the appointed password; range is from 1 to 16 characters
- State – the password showing, includes plain text and encrypted text. The plain text means that the content will be shown; the encrypted text means that the content will not be shown directly
- Operation – includes **Add** and **Delete**

Example 1: Select the FTP server state as **Open**, and type the FTP Timeout as **600** (seconds). Click **Apply** to complete the configuration.

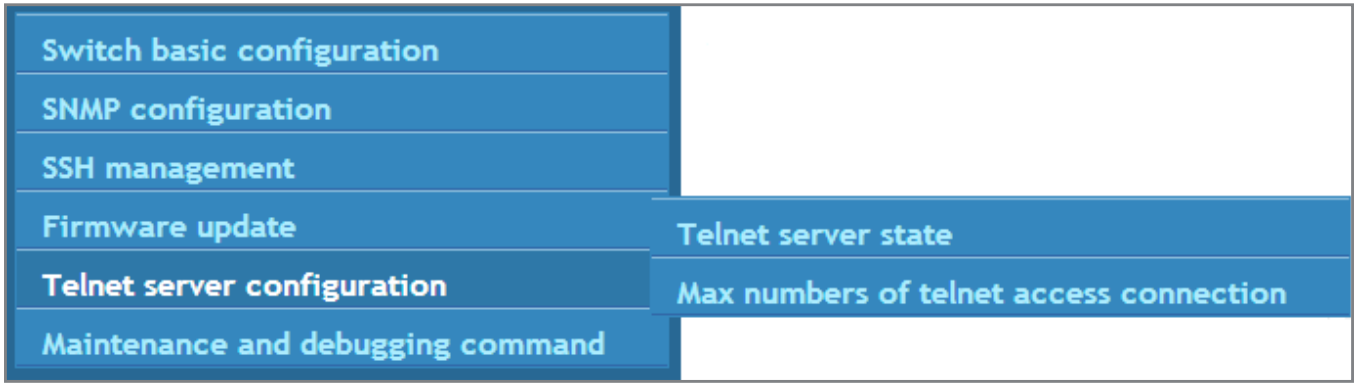


Example 2: Type the User name as **admin** and the Password as **switch**. Select the State as **Plain text** and Operation type as **Add**. Click **Apply** to complete the configuration. The configuration of the new user will be effective.



21.5 Telnet server configuration

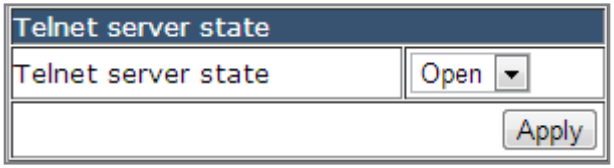
Click **Management->Telnet server configuration** to configure **Telnet server state** and **Max number of telnet access connections**.



21.5.1 Telnet server state

Click **Management->Telnet server configuration->Telnet server state** to configure.

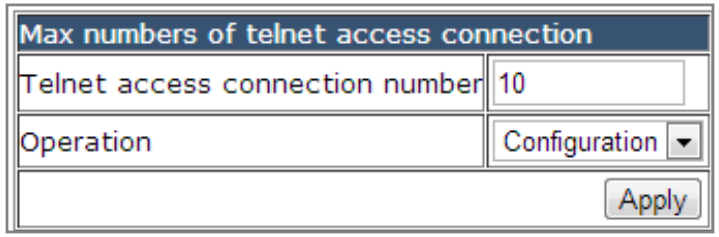
Example: Select the Telnet server state as **Open**, and then click **Apply** to start the Telnet server.



21.5.2 Max numbers of telnet access connection

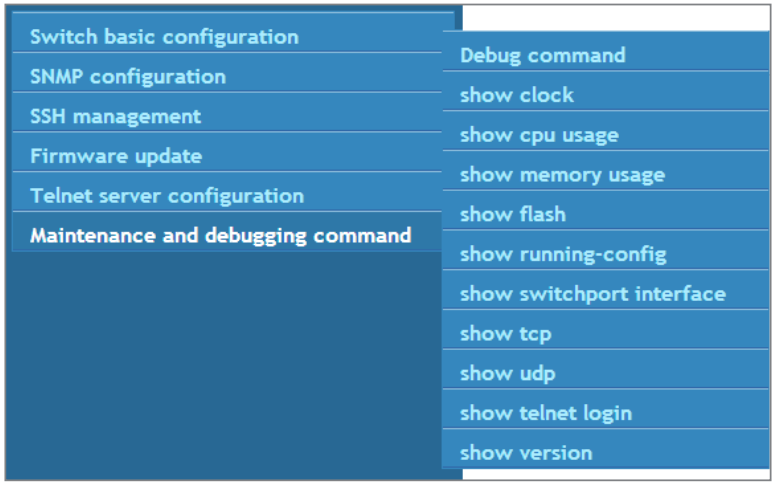
Click **Management->Telnet server configuration->Max Numbers of Telnet access connection** to configure.

Example: Type the Telnet access connection number as **10** and select Operation **Configuration**. Click **Apply** to complete the configuration.



21.6 Maintenance and debugging command

Click **Management-> Maintenance and debugging command** to open the configuration page.



The content includes:

- Debug command – the connection status of the tested switch
- show clock – the current time
- show CPU usage – the CPU usage information under the current running status
- show memory usage – the memory usage information under the current running status

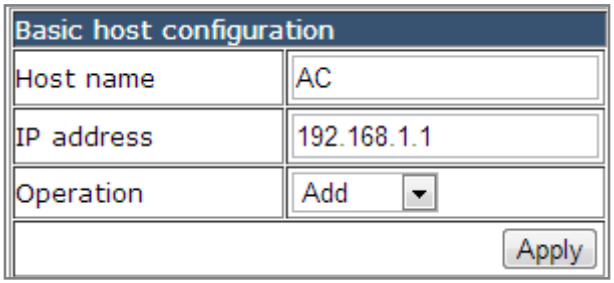
- show flash – the flash file information
- show running-configuration – the current parameters configuration
- show switchport interface – the property of the VLAN interface
- show tcp – the TCP that is currently connected to the switch
- show udp – the UDP that is currently connected to the switch
- show telnet login – the client information that is connected to the switch
- show version – the system version information of the switch

21.6.1 Debug command

Click **Management->Maintenance And Debugging Command->Debug Command** to open the **Configuration** page and configure basic host configuration, PING, and traceroute.

1. Basic configuration – configures the mapping between the switch and the IP address.

Example: Type the Host name as **AC** and the IP address as **192.168.1.1**. Select Operation **Add** and then click **Apply**.

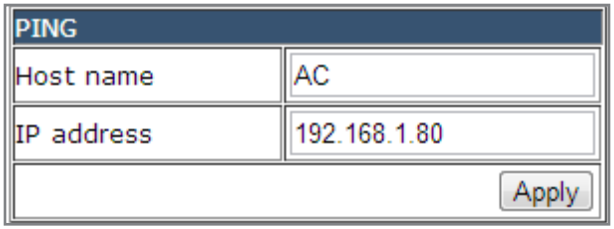


2. PING

The entries are as as follows:

- Host name – name of the host
- IP address – the destination IP address

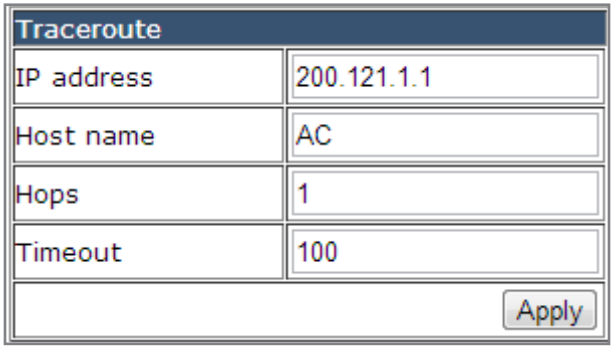
Example: Type the IP address as **192.168.1.80**, and then click **Apply**.



3. Traceroute

The entries are as follows:

- IP address – the destination IP address
- Host name – name of the host
- Hops – maximum number of hops
- Timeout – packet timeout



21.6.2 Others

The other configurations in the **Maintenance and Debugging Command** are simpler. Users can click the configuration tab to retrieve the corresponding information (they will not be listed one by one). Example:

1. Display the clock as follows:

```
Information feedback window
Current time is Sat Jun 22 19:25:58 2013
```

2. Display the CPU usage information under the current status as follows:

```
Information feedback window
Link1000ACS# show cpu usage
Last  5 second CPU IDLE:  96%
Last 30 second CPU IDLE:  95%
Last  5 minute CPU IDLE:  95%
From  running  CPU IDLE:  95%
```

3. Display the memory usage information under the current status as follows:

```
Information feedback window
Link1000ACS# show memory usage
The memory total 1024 MB , free 866361344 bytes , usage is 19.31%
```

4. Show the flash file as follows:

```
Information feedback window

-rwx        48              default_license.lic
-rwx        245             dh1024.pem
-rwx        156             dh512.pem
-rwx        14.6M           nos.img
-rwx        24              portal-locale.cfg
-rwx        3.0K            startup.cfg
-rwx        2.4K            test
-rwx        0               wlan.pem
-rwx        245             wsdh1024.pem
-rwx        156             wsdh512.pem
-rwx        928             wssl2_cert.pem
-rwx        912             wssl2_key.pem

Drive : flash:
Size:26.5M  Used:14.7M  Available:11.8M  Use:55%
```

Regulatory and compliance

The icXchange® Link1000ACS must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. This product contains encryption. It is unlawful to export out of the United States without obtaining a U.S. Export License.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate ICC's warranty and all applicable regulatory certifications and approvals.

Only antennas specified for your region by ICC can be used with this product. The use of external amplifiers or non-ICC antennas may invalidate regulatory certifications and approvals.

Declaration of ROHS compliance

International Communications Corporation hereby declares that the product icXchange® Link1000ACS access controller has been designed and manufactured in accordance with Directive 2002/95/EC of the European Commission on the restriction of certain hazardous substances in electrical and electronic equipment. (ROHS)

CAUTION: Exposure to radio frequency radiation

USA – Federal Communications Commission (FCC) EMC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful: The Interference Handbook. This booklet is available from the US Government Printing Office, Washington, DC 20402. Stock No. 004-000-0034504.

ICC is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this ICC Wireless 11b/g PoE Access Point, Model icXchange®, or the substitution or attachment of connecting cables and equipment other than specified by ICC.

The correction of interference caused by such unauthorized modification, substitution, or attachment will be the responsibility of the user.

Changes or modifications not expressly approved by ICC could void the user's authority to operate this equipment.

Manufacturer's FCC declaration of conformity

Model Number: Link1000ACS International Communications Corporation Equipment Type: Ethernet Switch

Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Safety compliance notice

This device has been tested and certified according to the following safety standards and is intended for use only in information technology equipment, which has been tested to these or other equivalent standards:

- EN60950-1
- IEC 60950-1
- UL 60950-1

Warranty

International Communications Corporation, Inc. (“ICC”), warrants its products to be free from defects in workmanship and materials, under normal use and service, starting from the date the original purchaser purchased the product (based on the invoice date on the authorized Partner’s invoice) from ICC or its Authorized reseller or distributor.

All icXchange® hardware, excluding fans and internal power supplies, is under warranty for the life of the product and 2 years after the product is End-of-Life. Fans and internal power supplies are not included in the lifetime warranty and are covered by a warranty period of five (5) years. Should any icXchange® product fail to function as warranted, ICC may, at its own discretion, either repair or replace the defective product with a similar or functionally equivalent product, during the applicable warranty period. ICC will endeavor to repair or replace any product returned under warranty within thirty (30) days of its receipt of the returned product. End-of-Life of a product is defined as the date that ICC no longer makes the product readily available for sale in its authorized channels. Support for icXchange® hardware can be extended via an icXchange® Service Contract.

ICC warrants that for a period of two (2) years from the invoice date on the authorized ICC distributor’s invoice that the Software supplied by ICC will perform substantially in accordance with the specifications set forth in the icXchange® user guide accompanying the Product. In the case of a defect, which is reproducible by ICC, the Software will be either repaired or replaced, at ICC’s option.

All products that are returned to ICC become the property of ICC. Repaired or replacement products may be refurbished or contain refurbished materials. Any replaced or repaired product carries the remainder of the initial warranty. ICC is not responsible for any Customer or custom software or firmware, configuration information or Customer memory data contained in, stored on, or integrated with any products returned to ICC pursuant to any warranty. Customer must back up or otherwise retain any such information or data prior to shipping product to ICC. Products returned to ICC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. ICC is not responsible for these items if they are returned to ICC with the product.

Prior to returning any defective product, Customers must contact ICC for a Return Material Authorization number (“RMA”). Proof of the original purchase may be required. Any product returned to ICC without a valid RMA number clearly marked on the outside of the package will be returned to the customer at customer’s expense. For warranty claims within the US and Canada, please call our toll-free customer support number at 1-855-692-7211. Customers are responsible for all shipping charges and risk of loss from their location to ICC. ICC is responsible for return shipping charges and risk of loss from ICC to customer’s location.

WARRANTIES EXCLUSIVE: IF AN ICC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER’S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT ICC’S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. PRODUCTS ARE NOT WARRANTED TO OPERATE UNINTERRUPTED OR ERROR FREE. ICC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. ICC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR IF IN ITS SOLE JUDGMENT THE ALLEGED DEFECT WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULLEST EXTENT ALLOWED BY LAW, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), ICC SHALL NOT BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF PROFIT, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF ICC OR ITS AUTHORIZED DISTRIBUTOR OR RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE MAXIMUM LIABILITY OF ICC UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THIS WARRANTY. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

http://www.intcomcorp.com

© 2014 International Communications Corporation, Inc. All Rights Reserved. Printed in U.S.A. Issue 1.0 9/15/14. icXchange is the registered trademark of International Communications Corporation,Inc. Acrobat Reader is a registered trademark of Adobe Systems, Inc. Mac OS is a registered trademark of Apple, Inc. Windows, Windows Server 2003, Windows Vista and Microsoft Internet Explorer are registered trademarks of Microsoft. Cisco is a registered trademark of Cisco, Inc. IBM is a registered trademark of International Business Machines Corporation. All other trademarks are property of their respective owners. Test results and examples are subject to unique business conditions, client IT environment, ICC products deployed, and other factors. These results may not be typical; your results may vary.